Caesar cipher

An example of a simple symmetric encryption scheme is the Caesar cipher

"If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others."

– Suetonius, Life of Julius Caesar

Caesar cipher

An example of a simple symmetric encryption scheme is the Caesar cipher

"If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others."

– Suetonius, Life of Julius Caesar

Each character of the plaintext is replaced with the character 3 positions down the alphabet, in a modular fashion

Caesar cipher

An example of a simple symmetric encryption scheme is the Caesar cipher

"If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others."

– Suetonius, Life of Julius Caesar

Each character of the plaintext is replaced with the character 3 positions down the alphabet, in a modular fashion

$$\begin{array}{cccccccccccccccccccccccccc}
\mathtt{A} & \mathtt{B} & \mathtt{C} & \mathtt{D} & \mathtt{E} & \mathtt{F} & \mathtt{G} & \mathtt{H} & \mathtt{I} & \mathtt{J} & \mathtt{K} & \mathtt{L} & \mathtt{M} & \mathtt{N} & \mathtt{O} & \mathtt{P} & \mathtt{Q} & \mathtt{R} & \mathtt{S} & \mathtt{T} & \mathtt{U} & \mathtt{V} & \mathtt{W} & \mathtt{X} & \mathtt{Y} & \mathtt{Z} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\mathtt{D} & \mathtt{E} & \mathtt{F} & \mathtt{G} & \mathtt{H} & \mathtt{I} & \mathtt{J} & \mathtt{K} & \mathtt{L} & \mathtt{M} & \mathtt{N} & \mathtt{O} & \mathtt{P} & \mathtt{Q} & \mathtt{R} & \mathtt{S} & \mathtt{T} & \mathtt{U} & \mathtt{V} & \mathtt{W} & \mathtt{X} & \mathtt{Y} & \mathtt{Z} & \mathtt{A} & \mathtt{B} & \mathtt{C}
\end{array}$$

Caesar cipher: example

$m =$ `A T T A C K A T D A W N`

$$\Big\downarrow \; \mathsf{Enc}(m)$$

Caesar cipher: example

$$m = \texttt{A T T A C K A T D A W N}$$

$$\big\downarrow \ \mathsf{Enc}(m)$$

$$c = \texttt{D W W D F N D W G D Z Q}$$

Caesar cipher: example

$$m = \texttt{A T T A C K A T D A W N}$$

$$\Big\downarrow \ \mathsf{Enc}(m)$$

$$c = \texttt{D W W D F N D W G D Z Q}$$

$$c = \texttt{U H W U H D W Q R Z}$$

$$\Big\downarrow \ \mathsf{Dec}(c)$$

$$m =$$

Caesar cipher: example

$m =$ A T T A C K A T D A W N

$$\downarrow \ \mathsf{Enc}(m)$$

$c =$ D W W D F N D W G D Z Q

$c =$ U H W U H D W Q R Z

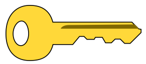
$$\downarrow \ \mathsf{Dec}(c)$$

$m =$ R E T R E A T N O W

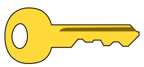
Shift ciphers

The Caesar cipher is a special type of *shift cipher*

In a shift cipher, each character is replaced with the character k positions down the alphabet (in a modular fashion)

The *key* of the cipher is the integer k 

(the key is also called the *shift* of the cipher)



$k = 5$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Shift ciphers

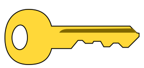
$m = \texttt{F L A N K T H E E N E M Y}$

$$\Big\downarrow\ \mathsf{Enc}_5(m)$$

$c = \texttt{K Q F S P Y M J J S J R D}$

$c = \texttt{X J S I M J Q U}$

$$\Big\downarrow\ \mathsf{Dec}_5(c)$$



$k = 5$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Shift ciphers

$$m = \texttt{F L A N K T H E E N E M Y}$$

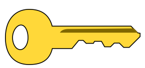
$$\Big\downarrow\ \mathsf{Enc}_5(m)$$

$$c = \texttt{K Q F S P Y M J J S J R D}$$

$$c = \texttt{X J S I M J Q U}$$

$$\Big\downarrow\ \mathsf{Dec}_5(c)$$

$$m = \texttt{S E N D H E L P}$$



$k = 5$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Shift ciphers

Message space: $\mathcal{M} = \{A, \ldots, Z\}^*$

Shift ciphers

Message space: $\mathcal{M} = \{0, 1, \ldots, 25\}^*$

Shift ciphers

Message space: $\mathcal{M} = \{0, 1, \ldots, 25\}^*$

Ciphertext space:

Shift ciphers

Message space: $\mathcal{M} = \{0, 1, \ldots, 25\}^*$

Ciphertext space: $\mathcal{C} = \{0, \ldots, 25\}^*$

Shift ciphers

Message space: $\mathcal{M} = \{0, 1, \ldots, 25\}^*$

Ciphertext space: $\mathcal{C} = \{0, \ldots, 25\}^*$

Key space:

Shift ciphers

Message space: $\mathcal{M} = \{0, 1, \ldots, 25\}^*$

Ciphertext space: $\mathcal{C} = \{0, \ldots, 25\}^*$

Key space: $\mathcal{K} = \{0, \ldots, 25\}$

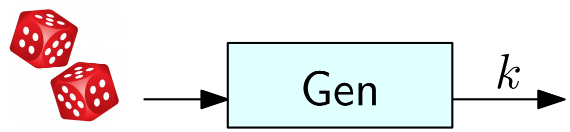
Shift ciphers

Message space: $\mathcal{M} = \{0, 1, \ldots, 25\}^*$

Ciphertext space: $\mathcal{C} = \{0, \ldots, 25\}^*$

Key space: $\mathcal{K} = \{0, \ldots, 25\}$

Key generation:



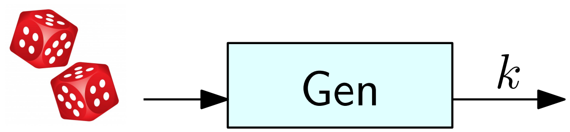
Shift ciphers

Message space: $\mathcal{M} = \{0, 1, \ldots, 25\}^*$

Ciphertext space: $\mathcal{C} = \{0, \ldots, 25\}^*$

Key space: $\mathcal{K} = \{0, \ldots, 25\}$

Key generation: return k chosen u.a.r. from $\mathcal{K}$



Shift ciphers

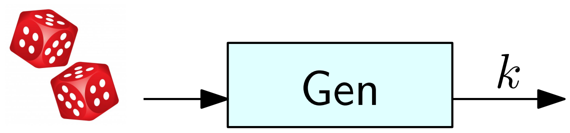
Message space: $\mathcal{M} = \{0, 1, \dots, 25\}^*$

$m = m_1 m_2 \dots m_\ell$

Ciphertext space: $\mathcal{C} = \{0, \dots, 25\}^*$

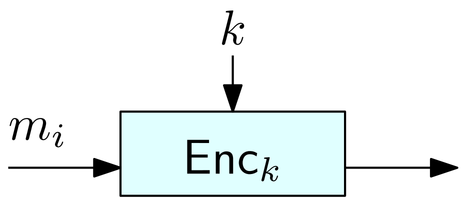
Key space: $\mathcal{K} = \{0, \dots, 25\}$

Key generation: return k chosen u.a.r. from $\mathcal{K}$



Encryption function:

$$\mathsf{Enc}_k(m) = \mathsf{Enc}_k(m_1) \| \mathsf{Enc}_k(m_2) \| \dots \| \mathsf{Enc}_k(m_\ell)$$



Shift ciphers

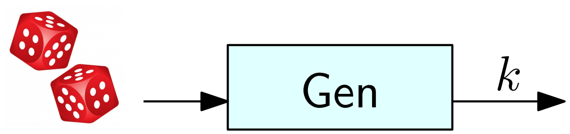
Message space: $\mathcal{M} = \{0, 1, \ldots, 25\}^*$

$m = m_1 m_2 \ldots m_\ell$

Ciphertext space: $\mathcal{C} = \{0, \ldots, 25\}^*$

Key space: $\mathcal{K} = \{0, \ldots, 25\}$

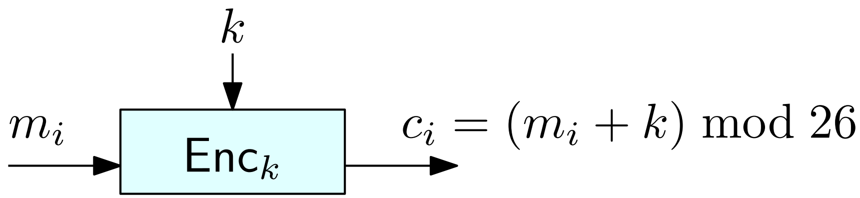
Key generation: return k chosen u.a.r. from $\mathcal{K}$



Encryption function:

$$\mathsf{Enc}_k(m) = \mathsf{Enc}_k(m_1) \| \mathsf{Enc}_k(m_2) \| \ldots \| \mathsf{Enc}_k(m_\ell)$$

$$\mathsf{Enc}_k(m_i) = (m_i + k) \bmod 26$$



Shift ciphers

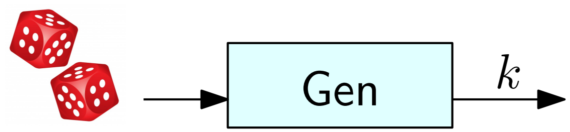
Message space: $\mathcal{M} = \{0, 1, \ldots, 25\}^*$

$$m = m_1 m_2 \ldots m_\ell$$
$$c = c_1 c_2 \ldots c_\ell$$

Ciphertext space: $\mathcal{C} = \{0, \ldots, 25\}^*$

Key space: $\mathcal{K} = \{0, \ldots, 25\}$

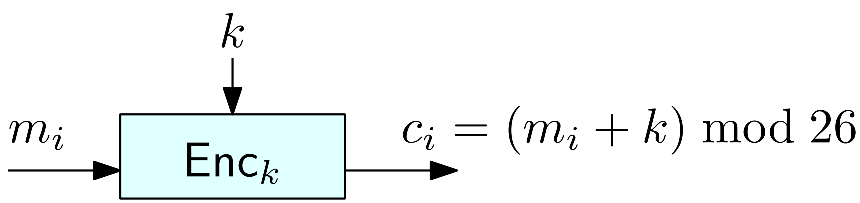
Key generation: return k chosen u.a.r. from $\mathcal{K}$



Encryption function:

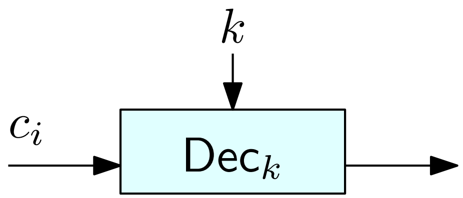
$$\mathsf{Enc}_k(m) = \mathsf{Enc}_k(m_1) \| \mathsf{Enc}_k(m_2) \| \ldots \| \mathsf{Enc}_k(m_\ell)$$

$$\mathsf{Enc}_k(m_i) = (m_i + k) \bmod 26$$



Decryption function:

$$\mathsf{Dec}_k(c) = \mathsf{Dec}_k(c_1) \| \mathsf{Dec}_k(c_2) \| \ldots \| \mathsf{Dec}_k(c_\ell)$$



Shift ciphers

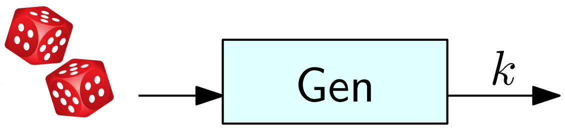
Message space: $\mathcal{M} = \{0, 1, \ldots, 25\}^*$

Ciphertext space: $\mathcal{C} = \{0, \ldots, 25\}^*$

Key space: $\mathcal{K} = \{0, \ldots, 25\}$

Key generation: return k chosen u.a.r. from $\mathcal{K}$

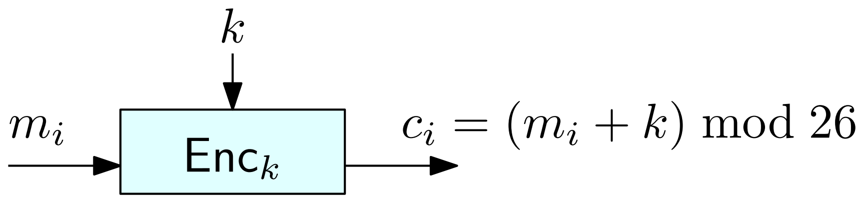
$$m = m_1 m_2 \ldots m_\ell$$
$$c = c_1 c_2 \ldots c_\ell$$



Encryption function:

$$\mathsf{Enc}_k(m) = \mathsf{Enc}_k(m_1) \| \mathsf{Enc}_k(m_2) \| \ldots \| \mathsf{Enc}_k(m_\ell)$$

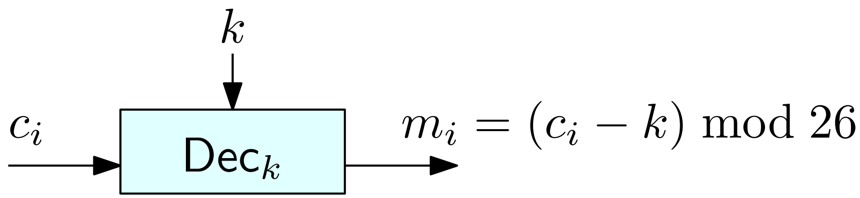
$$\mathsf{Enc}_k(m_i) = (m_i + k) \bmod 26$$



Decryption function:

$$\mathsf{Dec}_k(c) = \mathsf{Dec}_k(c_1) \| \mathsf{Dec}_k(c_2) \| \ldots \| \mathsf{Dec}_k(c_\ell)$$

$$\mathsf{Dec}_k(c_i) = (c_i - k) \bmod 26$$



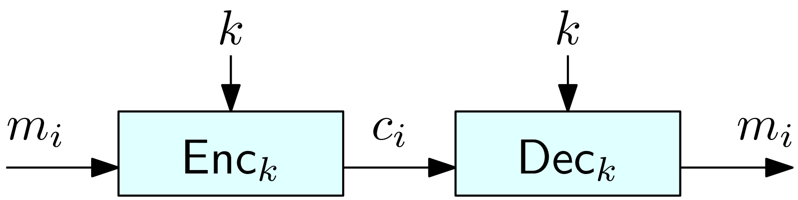
Shift ciphers

Correctness:

We need to prove that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$

Shift ciphers

Correctness:



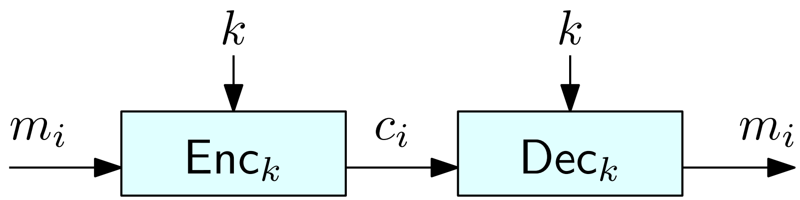
We need to prove that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$

It suffices to show that $\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) = m_i$

$\mathsf{Dec}_k(\mathsf{Enc}_k(m_i))$

Shift ciphers

Correctness:



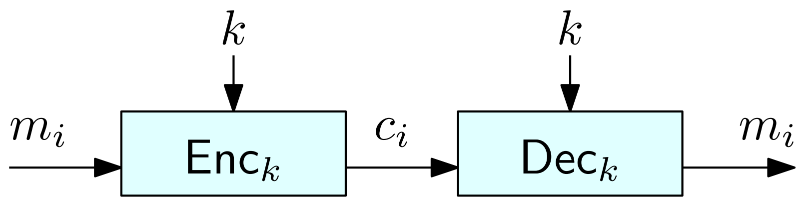
We need to prove that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$

It suffices to show that $\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) = m_i$

$\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) \ = \mathsf{Dec}_k((m_i + k) \bmod 26)$ (definition of Enc_k)

Shift ciphers

Correctness:



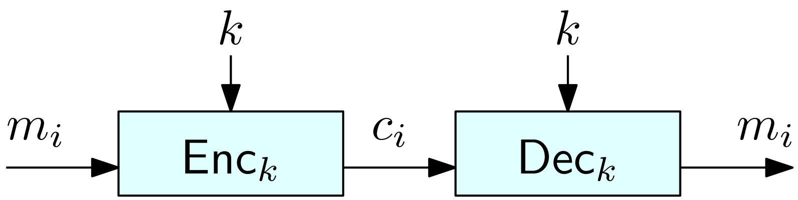
We need to prove that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$

It suffices to show that $\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) = m_i$

$$\begin{aligned}
\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) &= \mathsf{Dec}_k((m_i + k) \bmod 26) && \text{(definition of Enc}_k\text{)} \\
&= (((m_i + k) \bmod 26) - k) \bmod 26 && \text{(definition of Dec}_k\text{)}
\end{aligned}$$

Shift ciphers

Correctness:



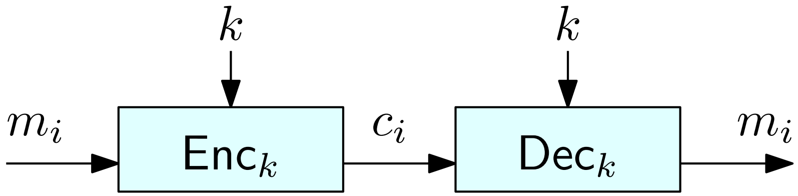
We need to prove that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$

It suffices to show that $\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) = m_i$

$$\begin{aligned}
\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) &= \mathsf{Dec}_k((m_i + k) \bmod 26) && \text{(definition of } \mathsf{Enc}_k\text{)} \\
&= (((m_i + k) \bmod 26) - k) \bmod 26 && \text{(definition of } \mathsf{Dec}_k\text{)} \\
&= (m_i + k - k) \bmod 26 && \text{(properties of } \mathrm{mod}\text{)}
\end{aligned}$$

Shift ciphers

Correctness:



We need to prove that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$

It suffices to show that $\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) = m_i$

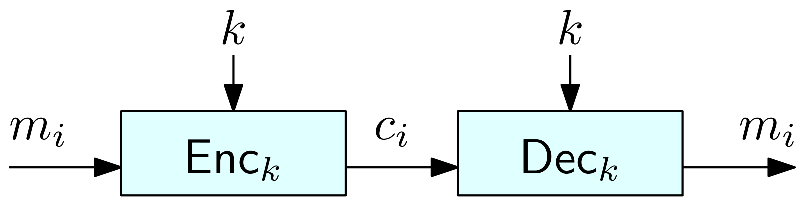
$$\begin{aligned}
\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) &= \mathsf{Dec}_k((m_i + k) \bmod 26) && \text{(definition of } \mathsf{Enc}_k\text{)} \\
&= (((m_i + k) \bmod 26) - k) \bmod 26 && \text{(definition of } \mathsf{Dec}_k\text{)} \\
&= (m_i + k - k) \bmod 26 && \text{(properties of } \mathrm{mod}\text{)} \\
&= m_i \bmod 26
\end{aligned}$$

Shift ciphers

Correctness:

We need to prove that $\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$

It suffices to show that $\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) = m_i$



$$
\begin{aligned}
\mathsf{Dec}_k(\mathsf{Enc}_k(m_i)) &= \mathsf{Dec}_k((m_i + k) \bmod 26) && \text{(definition of } \mathsf{Enc}_k\text{)} \\
&= (((m_i + k) \bmod 26) - k) \bmod 26 && \text{(definition of } \mathsf{Dec}_k\text{)} \\
&= (m_i + k - k) \bmod 26 && \text{(properties of } \mathrm{mod}\text{)} \\
&= m_i \bmod 26 \\
&= m_i && (m_i < 26)
\end{aligned}
$$

Shift ciphers

Are shift ciphers secure?

Shift ciphers

Are shift ciphers secure?

How many keys are there?

Shift ciphers

Are shift ciphers secure?

How many keys are there? $|\mathcal{K}| = 26$

Shift ciphers

Are shift ciphers secure?

How many keys are there? $|\mathcal{K}| = 26$

We can use a **brute-force** (or **exhaustive search**) attack

Shift ciphers

Are shift ciphers secure?

How many keys are there? $|\mathcal{K}| = 26$

We can use a **brute-force** (or **exhaustive search**) attack

In a brute-force attack, the adversary systematically tries all possible keys until the correct one is found.

Shift ciphers

Brute-force attack:

$$
\begin{aligned}
\mathsf{Dec}_0(c) &= \texttt{X J S I M J Q U} \\
\mathsf{Dec}_1(c) &= \texttt{W I R H L I P T} \\
\mathsf{Dec}_2(c) &= \texttt{V H Q G K H O S} \\
\mathsf{Dec}_3(c) &= \texttt{U G P F J G N R} \\
\mathsf{Dec}_4(c) &= \texttt{T F O E I F M Q} \\
\mathsf{Dec}_5(c) &= \texttt{S E N D H E L P} \\
\mathsf{Dec}_6(c) &= \texttt{R D M C G D K O} \\
&\vdots \\
\mathsf{Dec}_{24}(c) &= \texttt{Z L U K O L S W} \\
\mathsf{Dec}_{25}(c) &= \texttt{Y K T J N K R V}
\end{aligned}
$$

Shift ciphers

Brute-force attack:

$$\mathsf{Dec}_0(c) = \texttt{X J S I M J Q U}$$

$$\mathsf{Dec}_1(c) = \texttt{W I R H L I P T}$$

$$\mathsf{Dec}_2(c) = \texttt{V H Q G K H O S}$$

$$\mathsf{Dec}_3(c) = \texttt{U G P F J G N R}$$

$$\mathsf{Dec}_4(c) = \texttt{T F O E I F M Q}$$

$$\boxed{\mathsf{Dec}_5(c) = \texttt{S E N D H E L P}}$$

$$\mathsf{Dec}_6(c) = \texttt{R D M C G D K O}$$

$$\vdots$$

$$\mathsf{Dec}_{24}(c) = \texttt{Z L U K O L S W}$$

$$\mathsf{Dec}_{25}(c) = \texttt{Y K T J N K R V}$$

Shift ciphers

Brute-force attack:

$$\mathsf{Dec}_0(c) = \texttt{X J S I M J Q U}$$

$$\mathsf{Dec}_1(c) = \texttt{W I R H L I P T}$$

$$\mathsf{Dec}_2(c) = \texttt{V H Q G K H O S}$$

$$\mathsf{Dec}_3(c) = \texttt{U G P F J G N R}$$

$$\mathsf{Dec}_4(c) = \texttt{T F O E I F M Q}$$

$$\boxed{\mathsf{Dec}_5(c) = \texttt{S E N D H E L P}}$$

$$\mathsf{Dec}_6(c) = \texttt{R D M C G D K O}$$

$$\vdots$$

$$\mathsf{Dec}_{24}(c) = \texttt{Z L U K O L S W}$$

$$\mathsf{Dec}_{25}(c) = \texttt{Y K T J N K R V}$$

Sufficient key-space principle: Any cipher should use a “large enough” key space to prevent brute-force attacks

(Monoalphabetic) Substitution ciphers

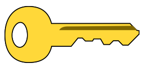
The key is now a permutation π of the alphabet $\Sigma = \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$

$\mathcal{K} = \{\pi : \Sigma \to \Sigma \mid \pi \text{ is a pemutation}\}$

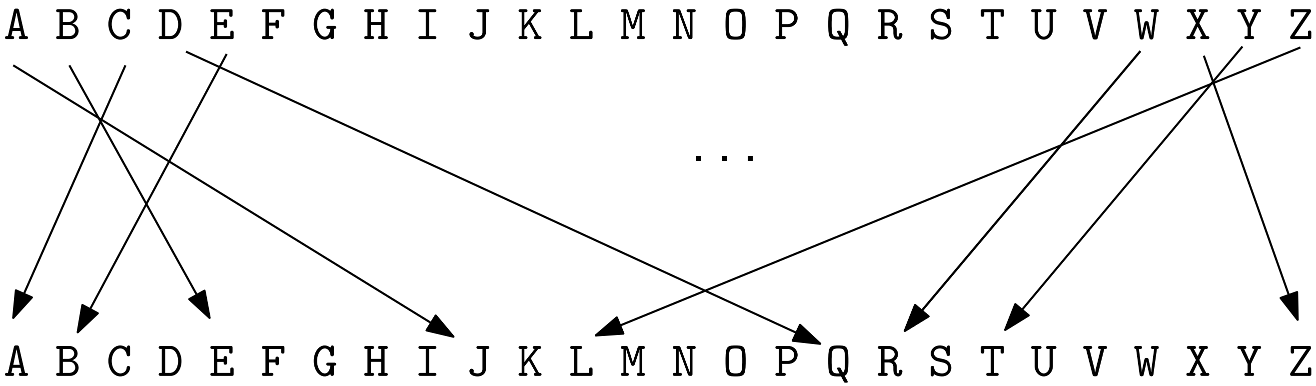
(Monoalphabetic) Substitution ciphers

The key is now a permutation π of the alphabet $\Sigma = \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$

$\mathcal{K} = \{\pi : \Sigma \to \Sigma \mid \pi \text{ is a pemutation}\}$



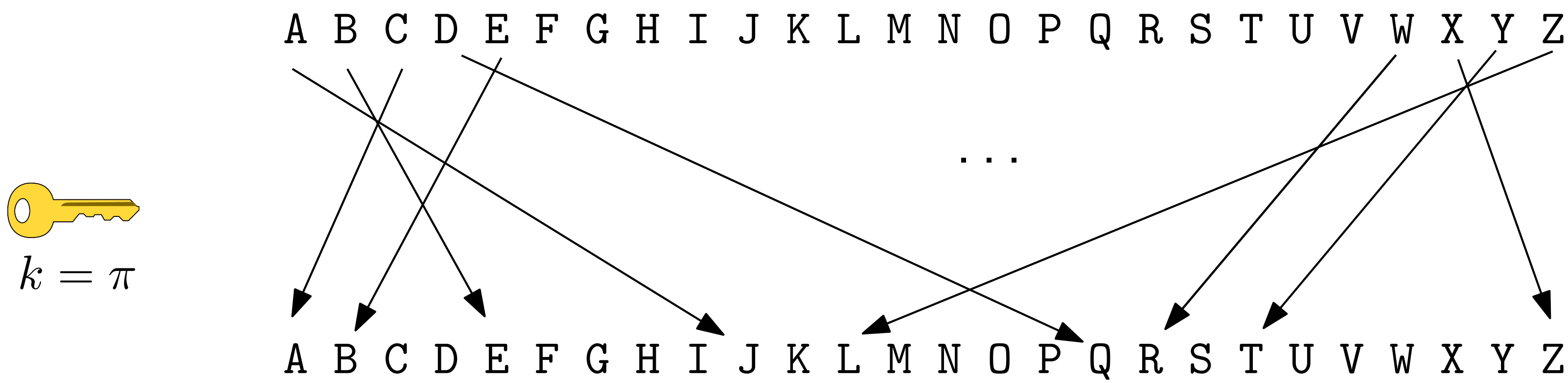
$k = \pi$



(Monoalphabetic) Substitution ciphers

The key is now a permutation π of the alphabet $\Sigma = \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$

$\mathcal{K} = \{\pi : \Sigma \to \Sigma \mid \pi \text{ is a pemutation}\}$



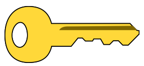
To encrypt a message, replace each character m_i in the plaintext with $k(m_i) = \pi(m_i)$

$\mathsf{Enc}_k(m) = k(m_1) \| k(m_2) \| \ldots \| k(m_\ell)$

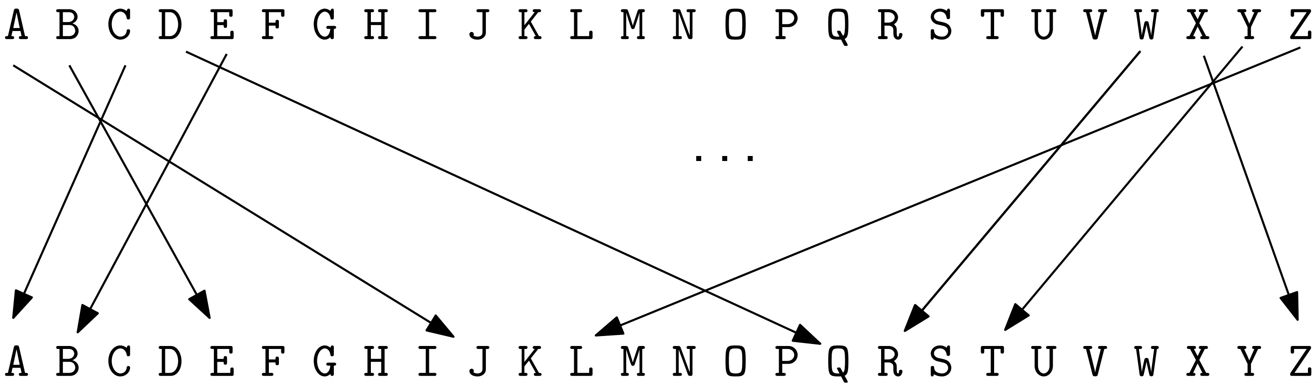
(Monoalphabetic) Substitution ciphers

The key is now a permutation π of the alphabet $\Sigma = \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$

$\mathcal{K} = \{\pi : \Sigma \to \Sigma \mid \pi \text{ is a pemutation}\}$



$k = \pi$



To encrypt a message, replace each character m_i in the plaintext with $k(m_i) = \pi(m_i)$

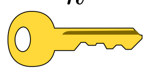
$\mathsf{Enc}_k(m) = k(m_1) \| k(m_2) \| \ldots \| k(m_\ell)$

To decrypt a message, replace each character c_i of the ciphertext with $k^{-1}(c_i) = \pi^{-1}(c_i)$

$\mathsf{Dec}_k(m) = k^{-1}(c_1) \| k^{-1}(c_2) \| \ldots \| k^{-1}(c_\ell)$

(Monoalphabetic) Substitution ciphers

$$\underbrace{\begin{array}{cccccccccccccccccccccccccc}
\mathtt{A} & \mathtt{B} & \mathtt{C} & \mathtt{D} & \mathtt{E} & \mathtt{F} & \mathtt{G} & \mathtt{H} & \mathtt{I} & \mathtt{J} & \mathtt{K} & \mathtt{L} & \mathtt{M} & \mathtt{N} & \mathtt{O} & \mathtt{P} & \mathtt{Q} & \mathtt{R} & \mathtt{S} & \mathtt{T} & \mathtt{U} & \mathtt{V} & \mathtt{W} & \mathtt{X} & \mathtt{Y} & \mathtt{Z} \\
\mathtt{J} & \mathtt{E} & \mathtt{A} & \mathtt{Q} & \mathtt{B} & \mathtt{Y} & \mathtt{D} & \mathtt{P} & \mathtt{V} & \mathtt{F} & \mathtt{K} & \mathtt{I} & \mathtt{N} & \mathtt{H} & \mathtt{M} & \mathtt{X} & \mathtt{U} & \mathtt{S} & \mathtt{W} & \mathtt{C} & \mathtt{O} & \mathtt{G} & \mathtt{R} & \mathtt{Z} & \mathtt{T} & \mathtt{L}
\end{array}}_{k}$$



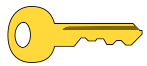
$$m = \mathtt{A\ W\ A\ I\ T\ O\ R\ D\ E\ R\ S}$$

$$\Big\downarrow \; \mathsf{Enc}_k(m)$$

(Monoalphabetic) Substitution ciphers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	E	A	Q	B	Y	D	P	V	F	K	I	N	H	M	X	U	S	W	C	O	G	R	Z	T	L

k



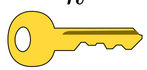
$$m = \texttt{A W A I T O R D E R S}$$

$$\big\downarrow \ \mathsf{Enc}_k(m)$$

$$c = \texttt{J R J V C M S Q B S W}$$

(Monoalphabetic) Substitution ciphers

$$\underbrace{\begin{array}{cccccccccccccccccccccccccc} \mathtt{A} & \mathtt{B} & \mathtt{C} & \mathtt{D} & \mathtt{E} & \mathtt{F} & \mathtt{G} & \mathtt{H} & \mathtt{I} & \mathtt{J} & \mathtt{K} & \mathtt{L} & \mathtt{M} & \mathtt{N} & \mathtt{O} & \mathtt{P} & \mathtt{Q} & \mathtt{R} & \mathtt{S} & \mathtt{T} & \mathtt{U} & \mathtt{V} & \mathtt{W} & \mathtt{X} & \mathtt{Y} & \mathtt{Z} \\ \mathtt{J} & \mathtt{E} & \mathtt{A} & \mathtt{Q} & \mathtt{B} & \mathtt{Y} & \mathtt{D} & \mathtt{P} & \mathtt{V} & \mathtt{F} & \mathtt{K} & \mathtt{I} & \mathtt{N} & \mathtt{H} & \mathtt{M} & \mathtt{X} & \mathtt{U} & \mathtt{S} & \mathtt{W} & \mathtt{C} & \mathtt{O} & \mathtt{G} & \mathtt{R} & \mathtt{Z} & \mathtt{T} & \mathtt{L} \end{array}}_{k}$$



$m = \mathtt{A\ W\ A\ I\ T\ O\ R\ D\ E\ R\ S}$

$\big\downarrow\ \mathsf{Enc}_k(m)$

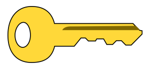
$c = \mathtt{J\ R\ J\ V\ C\ M\ S\ Q\ B\ S\ W}$

$c = \mathtt{B\ H\ B\ N\ T\ Q\ M\ R\ H}$

$\big\downarrow\ \mathsf{Dec}_k(c)$

(Monoalphabetic) Substitution ciphers

$$\underbrace{\begin{array}{cccccccccccccccccccccccccc}
\mathtt{A} & \mathtt{B} & \mathtt{C} & \mathtt{D} & \mathtt{E} & \mathtt{F} & \mathtt{G} & \mathtt{H} & \mathtt{I} & \mathtt{J} & \mathtt{K} & \mathtt{L} & \mathtt{M} & \mathtt{N} & \mathtt{O} & \mathtt{P} & \mathtt{Q} & \mathtt{R} & \mathtt{S} & \mathtt{T} & \mathtt{U} & \mathtt{V} & \mathtt{W} & \mathtt{X} & \mathtt{Y} & \mathtt{Z} \\
\mathtt{J} & \mathtt{E} & \mathtt{A} & \mathtt{Q} & \mathtt{B} & \mathtt{Y} & \mathtt{D} & \mathtt{P} & \mathtt{V} & \mathtt{F} & \mathtt{K} & \mathtt{I} & \mathtt{N} & \mathtt{H} & \mathtt{M} & \mathtt{X} & \mathtt{U} & \mathtt{S} & \mathtt{W} & \mathtt{C} & \mathtt{O} & \mathtt{G} & \mathtt{R} & \mathtt{Z} & \mathtt{T} & \mathtt{L}
\end{array}}_{k}$$



$$m = \mathtt{A\ W\ A\ I\ T\ O\ R\ D\ E\ R\ S}$$

$$\Big\downarrow \ \mathsf{Enc}_k(m)$$

$$c = \mathtt{J\ R\ J\ V\ C\ M\ S\ Q\ B\ S\ W}$$

$$c = \mathtt{B\ H\ B\ N\ T\ Q\ M\ R\ H}$$

$$\Big\downarrow \ \mathsf{Dec}_k(c)$$

$$m = \mathtt{E\ N\ E\ M\ Y\ D\ O\ W\ N}$$

(Monoalphabetic) Substitution ciphers

How many keys are there?

(Monoalphabetic) Substitution ciphers

How many keys are there?

$|K| = |\Sigma|! = 26! \approx 2^{88}$

(Monoalphabetic) Substitution ciphers

How many keys are there?

$|K| = |\Sigma|! = 26! \approx 2^{88}$

Is a brute-force attack feasible?

(Monoalphabetic) Substitution ciphers

How many keys are there?

$|K| = |\Sigma|! = 26! \approx 2^{88}$

Is a brute-force attack feasible? **No**

If we tried 100 billion keys per second, we would need about 100 million years to find the right permutation k

(Monoalphabetic) Substitution ciphers

How many keys are there?

$|K| = |\Sigma|! = 26! \approx 2^{88}$

Is a brute-force attack feasible? **No**

If we tried 100 billion keys per second, we would need about
100 million years to find the right permutation k

Are permutation ciphers secure?

(Monoalphabetic) Substitution ciphers

How many keys are there?

$|K| = |\Sigma|! = 26! \approx 2^{88}$

Is a brute-force attack feasible? **No**

If we tried 100 billion keys per second, we would need about 100 million years to find the right permutation k

Are permutation ciphers secure?

- They are resistant to brute-force attacks

(Monoalphabetic) Substitution ciphers

How many keys are there?

$|K| = |\Sigma|! = 26! \approx 2^{88}$

Is a brute-force attack feasible? **No**

If we tried 100 billion keys per second, we would need about
100 million years to find the right permutation k

Are permutation ciphers secure?

- They are resistant to brute-force attacks
- ... but they might be susceptible to more sophisticated attack techniques

(Monoalphabetic) Substitution ciphers

How many keys are there?

$|K| = |\Sigma|! = 26! \approx 2^{88}$

Is a brute-force attack feasible? **No**

If we tried 100 billion keys per second, we would need about
100 million years to find the right permutation k

Are permutation ciphers secure?

- They are resistant to brute-force attacks
- ... but they might be susceptible to more sophisticated attack techniques

Observation (informal): A large keyspace is not a sufficient condition for a cipher to be secure

Substitution ciphers

Suppose that we somehow have deciphered a small portion of the ciphertext

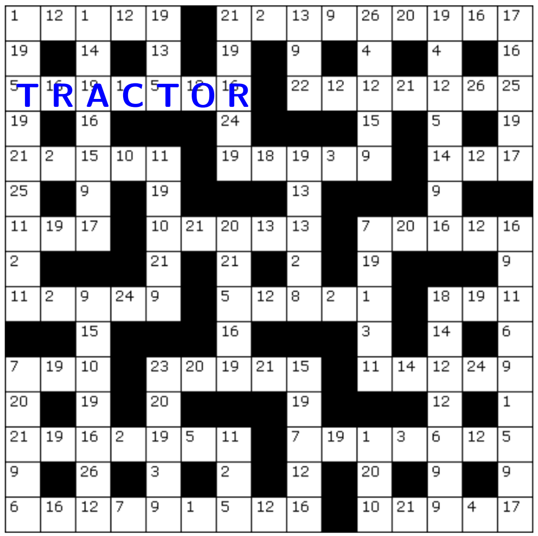
We can replace each known ciphertext symbol x with its plaintext $k^{-1}(x)$ and then use the partially decrypted message to make further guesses about k

Substitution ciphers

Suppose that we somehow have deciphered a small portion of the ciphertext

We can replace each known ciphertext symbol x with its plaintext $k^{-1}(x)$ and then use the partially decrypted message to make further guesses about k

A similar example: codebreaker word puzzle



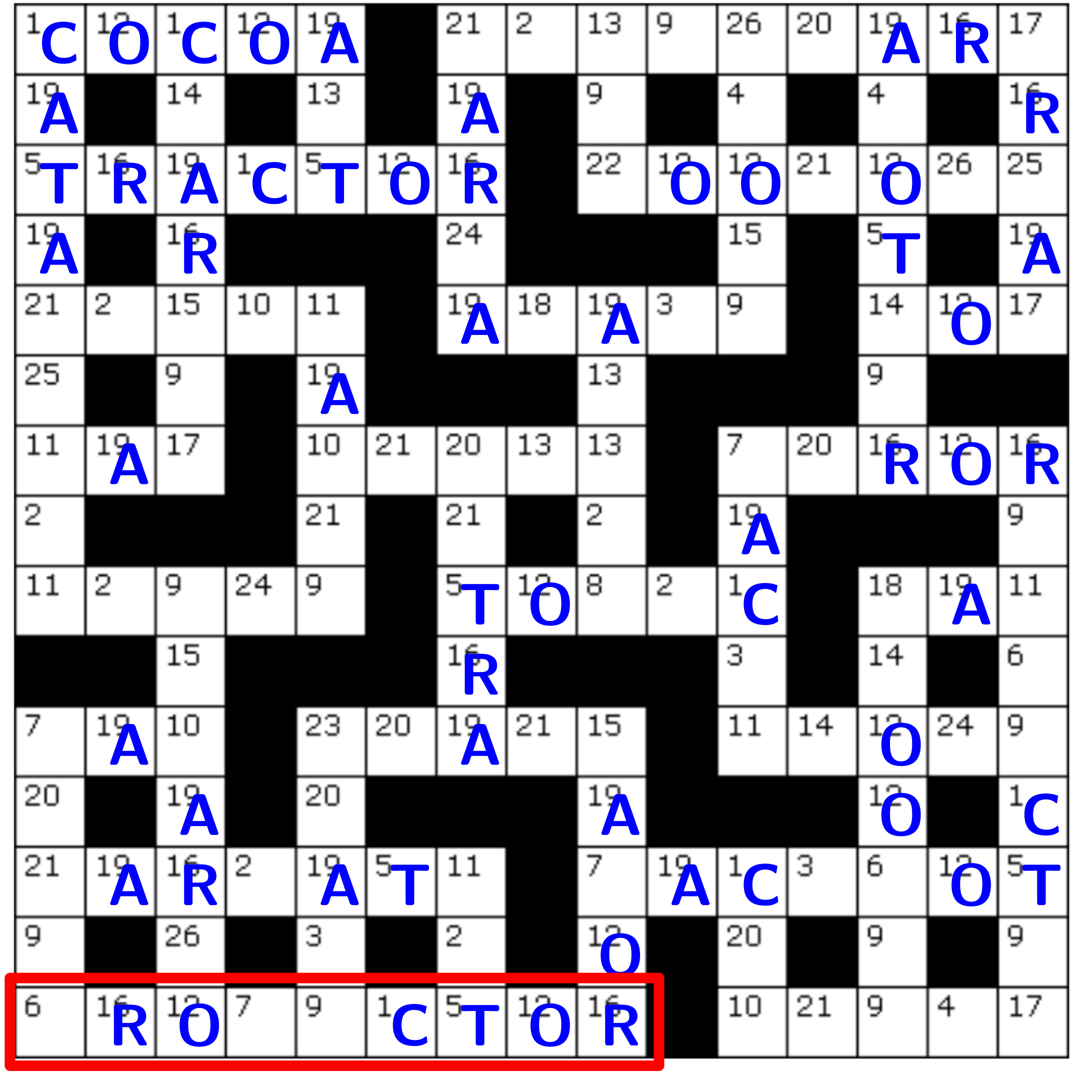
Substitution ciphers

1	12	1	12	19		21	2	13	9	26	20	19	16	17
19		14		13		19		9		4		4		16
5 T	16 R	19 A	1 C	5 T	12 O	16 R		22	12	12	21	12	26	25
19		16				24				15		5		19
21	2	15	10	11		19	18	19	3	9		14	12	17
25		9		19				13				9		
11	19	17		10	21	20	13	13		7	20	16	12	16
2				21		21		2		19				9
11	2	9	24	9		5	12	8	2	1		18	19	11
		15				16				3		14		6
7	19	10		23	20	19	21	15		11	14	12	24	9
20		19		20				19				12		1
21	19	16	2	19	5	11		7	19	1	3	6	12	5
9		26		3		2		12		20		9		9
6	16	12	7	9	1	5	12	16		10	21	9	4	17

Substitution ciphers

1 C	12 O	1 C	12 O	19 A		21	2	13	9	26	20	19 A	16 R	17
19 A		14		13		19 A		9		4		4		16 R
5 T	16 R	19 A	1 C	5 T	12 O	16 R		22	12 O	12 O	21	12 O	26	25
19 A		16 R				24				15		5 T		19 A
21	2	15	10	11		19 A	18	19 A	3	9		14	12 O	17
25		9		19 A				13				9		
11	19 A	17		10	21	20	13	13		7	20	16 R	12 O	16 R
2				21		21		2		19 A				9
11	2	9	24	9		5 T	12 O	8	2	1 C		18	19 A	11
		15				16 R				3		14		6
7	19 A	10		23	20	19 A	21	15		11	14	12 O	24	9
20		19 A		20				19 A				12 O		1 C
21	19 A	16 R	2	19 A	5 T	11		7	19 A	1 C	3	6	12 O	5 T
9		26		3		2		12 O		20		9		9
6	16 R	12 O	7	9	1 C	5 T	12 O	16 R		10	21	9	4	17

Substitution ciphers



Substitution ciphers

Substitution ciphers

Substitution ciphers

1 C	12 O	1 C	12 O	19 A	■	21	2	13	9 E	26	20	19 A	16 R	17 D
19 A	■	14	■	13	■	19 A	■	9 E	■	4	■	4	■	16 R
5 T	16 R	19 A	1 C	5 T	12 O	16 R	■	22	12 O	12 O	21	12 O	26	25
19 A	■	16 R	■	■	■	24	■	■	■	15	■	5 T	■	19 A
21	2	15	10	11 S	■	19 A	18	19 A	3	9 E	■	14	12 O	17 D
25	■	9 E	■	19 A	■	■	■	13	■	■	■	9 E	■	■
11 S	19 A	17	■	10	21	20	13	13	■	7 J	20	16 R	12 O	16 R
2	■	■	■	21	■	21	■	2	■	19 A	■	■	■	9 E
11 S	2	9 E	24	9 E	■	5 T	12 O	8	2	1 C	■	18	19 A	11 S
■	■	15	■	■	■	16 R	■	■	■	3	■	14	■	6 P
7 J	19 A	10	■	23	20	19 A	21	15	■	11 S	14	12 O	24	9 E
20	■	19 A	■	20	■	■	■	19 A	■	■	■	12 O	■	1 C
21	19 A	16 R	2	19 A	5 T	11 S	■	7 J	19 A	1 C	3	6 P	12 O	5 T
9 E	■	26	■	3	■	2	■	12 O	■	20	■	9 E	■	9 E
6 P	16 R	12 O	7 J	9 E	1 C	5 T	12 O	16 R	■	10	21	9 E	4	17 D

Substitution ciphers

Substitution ciphers

1 C	12 O	1 C	12 O	19 A		21	2	13	9 E	26	20 U	19 A	16 R	17 D
19 A		14		13		19 A		9 E		4		4		16 R
5 T	16 R	19 A	1 C	5 T	12 O	16 R		22	12 O	12 O	21	12 O	26	25
19 A		16 R				24				15		5 T		19 A
21	2	15	10	11 S		19 A	18	19 A	3	9 E		14	12 O	17 D
25		9 E		19 A				13				9 E		
11 S	19 A	17		10	21	20 U	13	13		7 J	20 U	16 R	12 O	16 R
2				21		21		2		19 A				9 E
11 S	2	9 E	24	9 E		5 T	12 O	8	2	1 C		18	19 A	11 S
		15				16 R				3		14		6 P
7 J	19 A	10		23	20 U	19 A	21	15		11 S	14	12 O	24	9 E
20 U		19 A		20 U				19 A				12 O		1 C
21	19 A	16 R	2	19 A	5 T	11 S		7 J	19 A	1 C	3	6 P	12 O	5 T
9 E		26		3		2		12 O		20 U		9 E		9 E
6 P	16 R	12 O	7 J	9 E	1 C	5 T	12 O	16 R		10	21	9 E	4	17 D

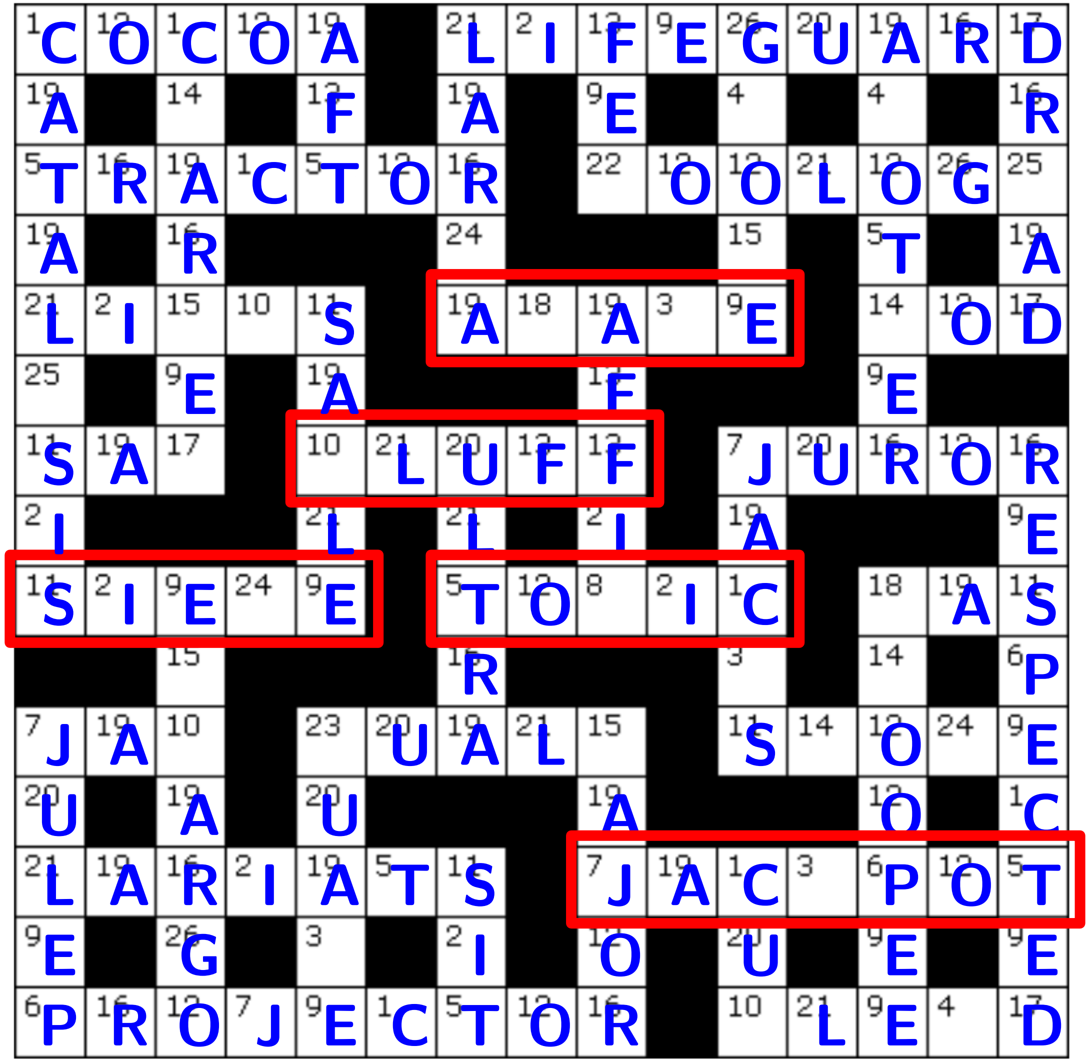
Substitution ciphers

1 C	12 O	1 C	12 O	19 A	■	21	2	13	9 E	26	20 U	19 A	16 R	17 D
19 A	■	14	■	13	■	19 A	■	9 E	■	4	■	4	■	16 R
5 T	16 R	19 A	1 C	5 T	12 O	16 R	■	22	12 O	12 O	21	12 O	26	25
19 A	■	16 R	■	■	■	24	■	■	■	15	■	5 T	■	19 A
21	2	15	10	11 S	■	19 A	18	19 A	3	9 E	■	14	12 O	17 D
25	■	9 E	■	19 A	■	■	■	13	■	■	■	9 E	■	■
11 S	19 A	17	■	10	21	20 U	13	13	■	7 J	20 U	16 R	12 O	16 R
2	■	■	■	21	■	21	■	2	■	19 A	■	■	■	9 E
11 S	2	9 E	24	9 E	■	5 T	12 O	8	2	1 C	■	18	19 A	11 S
■	■	15	■	■	■	16 R	■	■	■	3	■	14	■	6 P
7 J	19 A	10	■	23	20 U	19 A	21	15	■	11 S	14	12 O	24	9 E
20 U	■	19 A	■	20 U	■	■	■	19 A	■	■	■	12 O	■	1 C
21	19 A	16 R	2	19 A	5 T	11 S	■	7 J	19 A	1 C	3	6 P	12 O	5 T
9 E	■	26	■	3	■	2	■	12 O	■	20 U	■	9 E	■	9 E
6 P	16 R	12 O	7 J	9 E	1 C	5 T	12 O	16 R	■	10	21	9 E	4	17 D

Substitution ciphers

1 C	12 O	1 C	12 O	19 A	■	21 L	2 I	13 F	9 E	26 G	20 U	19 A	16 R	17 D
19 A	■	14	■	13 F	■	19 A	■	9 E	■	4	■	4	■	16 R
5 T	16 R	19 A	1 C	5 T	12 O	16 R	■	22	12 O	12 O	21 L	12 O	26 G	25
19 A	■	16 R	■	■	■	24	■	■	■	15	■	5 T	■	19 A
21 L	2 I	15	10	11 S	■	19 A	18	19 A	3	9 E	■	14	12 O	17 D
25	■	9 E	■	19 A	■	■	■	13 F	■	■	■	9 E	■	■
11 S	19 A	17	■	10	21 L	20 U	13 F	13 F	■	7 J	20 U	16 R	12 O	16 R
2 I	■	■	■	21 L	■	21 L	■	2 I	■	19 A	■	■	■	9 E
11 S	2 I	9 E	24	9 E	■	5 T	12 O	8	2 I	1 C	■	18	19 A	11 S
■	■	15	■	■	■	16 R	■	■	■	3	■	14	■	6 P
7 J	19 A	10	■	23	20 U	19 A	21 L	15	■	11 S	14	12 O	24	9 E
20 U	■	19 A	■	20 U	■	■	■	19 A	■	■	■	12 O	■	1 C
21 L	19 A	16 R	2 I	19 A	5 T	11 S	■	7 J	19 A	1 C	3	6 P	12 O	5 T
9 E	■	26 G	■	3	■	2 I	■	12 O	■	20 U	■	9 E	■	9 E
6 P	16 R	12 O	7 J	9 E	1 C	5 T	12 O	16 R	■	10	21 L	9 E	4	17 D

Substitution ciphers



Substitution ciphers

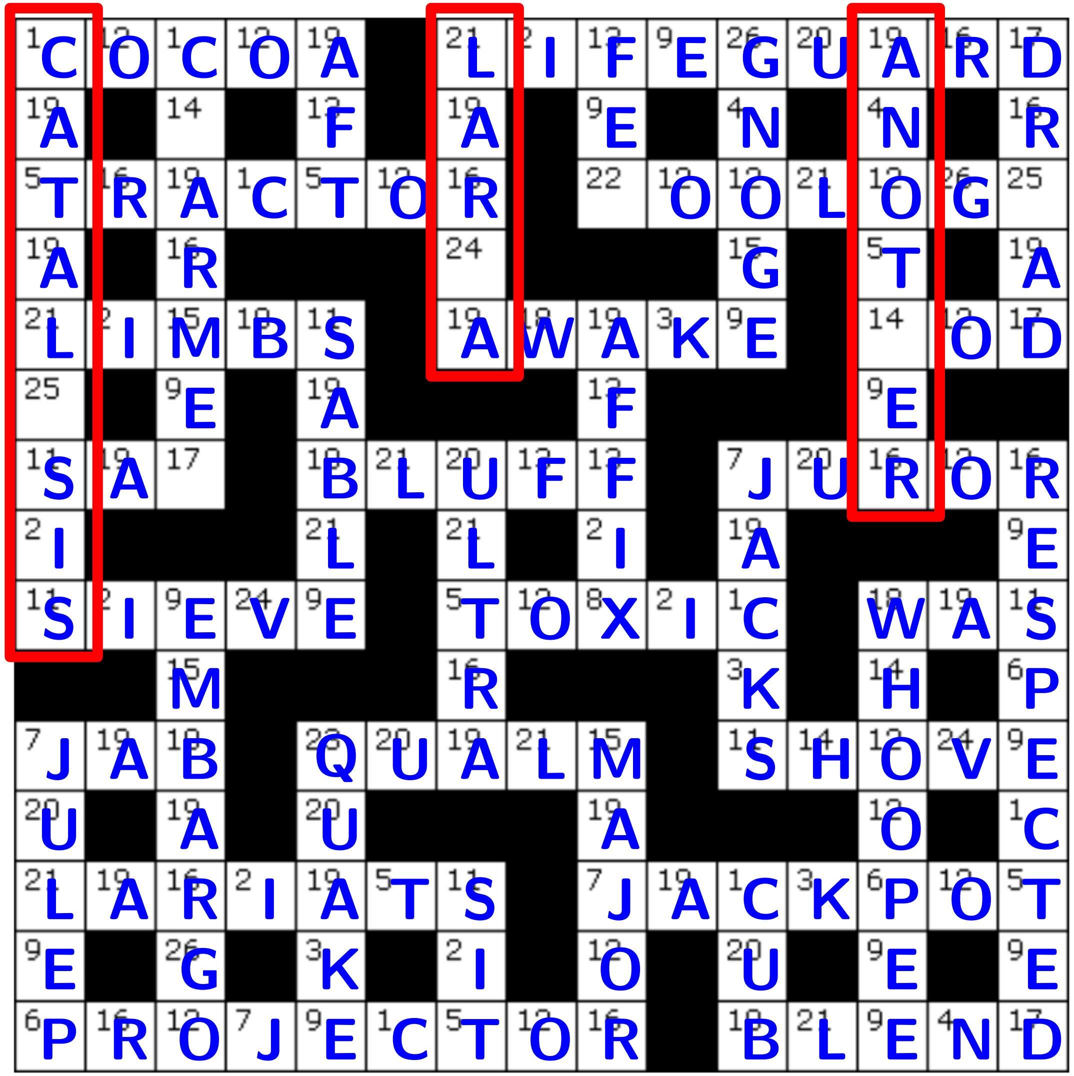
1 C	12 O	1 C	12 O	19 A	■	21 L	2 I	13 F	9 E	26 G	20 U	19 A	16 R	17 D
19 A	■	14	■	13 F	■	19 A	■	9 E	■	4	■	4	■	16 R
5 T	16 R	19 A	1 C	5 T	12 O	16 R	■	22	12 O	12 O	21 L	12 O	26 G	25
19 A	■	16 R	■	■	■	24	■	■	■	15	■	5 T	■	19 A
21 L	2 I	15	10 B	11 S	■	19 A	18 W	19 A	3 K	9 E	■	14	12 O	17 D
25	■	9 E	■	19 A	■	■	■	13 F	■	■	■	9 E	■	■
11 S	19 A	17	■	10 B	21 L	20 U	13 F	13 F	■	7 J	20 U	16 R	12 O	16 R
2 I	■	■	■	21 L	■	21 L	■	2 I	■	19 A	■	■	■	9 E
11 S	2 I	9 E	24 V	9 E	■	5 T	12 O	8 X	2 I	1 C	■	18 W	19 A	11 S
■	■	15	■	■	■	16 R	■	■	■	3 K	■	14	■	6 P
7 J	19 A	10 B	■	23	20 U	19 A	21 L	15	■	11 S	14	12 O	24 V	9 E
20 U	■	19 A	■	20 U	■	■	■	19 A	■	■	■	12 O	■	1 C
21 L	19 A	16 R	2 I	19 A	5 T	11 S	■	7 J	19 A	1 C	3 K	6 P	12 O	5 T
9 E	■	26 G	■	3 K	■	2 I	■	12 O	■	20 U	■	9 E	■	9 E
6 P	16 R	12 O	7 J	9 E	1 C	5 T	12 O	16 R	■	10 B	21 L	9 E	4	17 D

Substitution ciphers

Substitution ciphers

1 C	12 O	1 C	12 O	19 A	■	21 L	2 I	13 F	9 E	26 G	20 U	19 A	16 R	17 D
19 A	■	14	■	13 F	■	19 A	■	9 E	■	4 N	■	4 N	■	16 R
5 T	16 R	19 A	1 C	5 T	12 O	16 R	■	22	12 O	12 O	21 L	12 O	26 G	25
19 A	■	16 R	■	■	■	24	■	■	■	15 G	■	5 T	■	19 A
21 L	2 I	15 M	10 B	11 S	■	19 A	18 W	19 A	3 K	9 E	■	14	12 O	17 D
25	■	9 E	■	19 A	■	■	■	13 F	■	■	■	9 E	■	■
11 S	19 A	17	■	10 B	21 L	20 U	13 F	13 F	■	7 J	20 U	16 R	12 O	16 R
2 I	■	■	■	21 L	■	21 L	■	2 I	■	19 A	■	■	■	9 E
11 S	2 I	9 E	24 V	9 E	■	5 T	12 O	8 X	2 I	1 C	■	18 W	19 A	11 S
■	■	15 M	■	■	■	16 R	■	■	■	3 K	■	14 H	■	6 P
7 J	19 A	10 B	■	23 Q	20 U	19 A	21 L	15 M	■	11 S	14 H	12 O	24 V	9 E
20 U	■	19 A	■	20 U	■	■	■	19 A	■	■	■	12 O	■	1 C
21 L	19 A	16 R	2 I	19 A	5 T	11 S	■	7 J	19 A	1 C	3 K	6 P	12 O	5 T
9 E	■	26 G	■	3 K	■	2 I	■	12 O	■	20 U	■	9 E	■	9 E
6 P	16 R	12 O	7 J	9 E	1 C	5 T	12 O	16 R	■	10 B	21 L	9 E	4 N	17 D

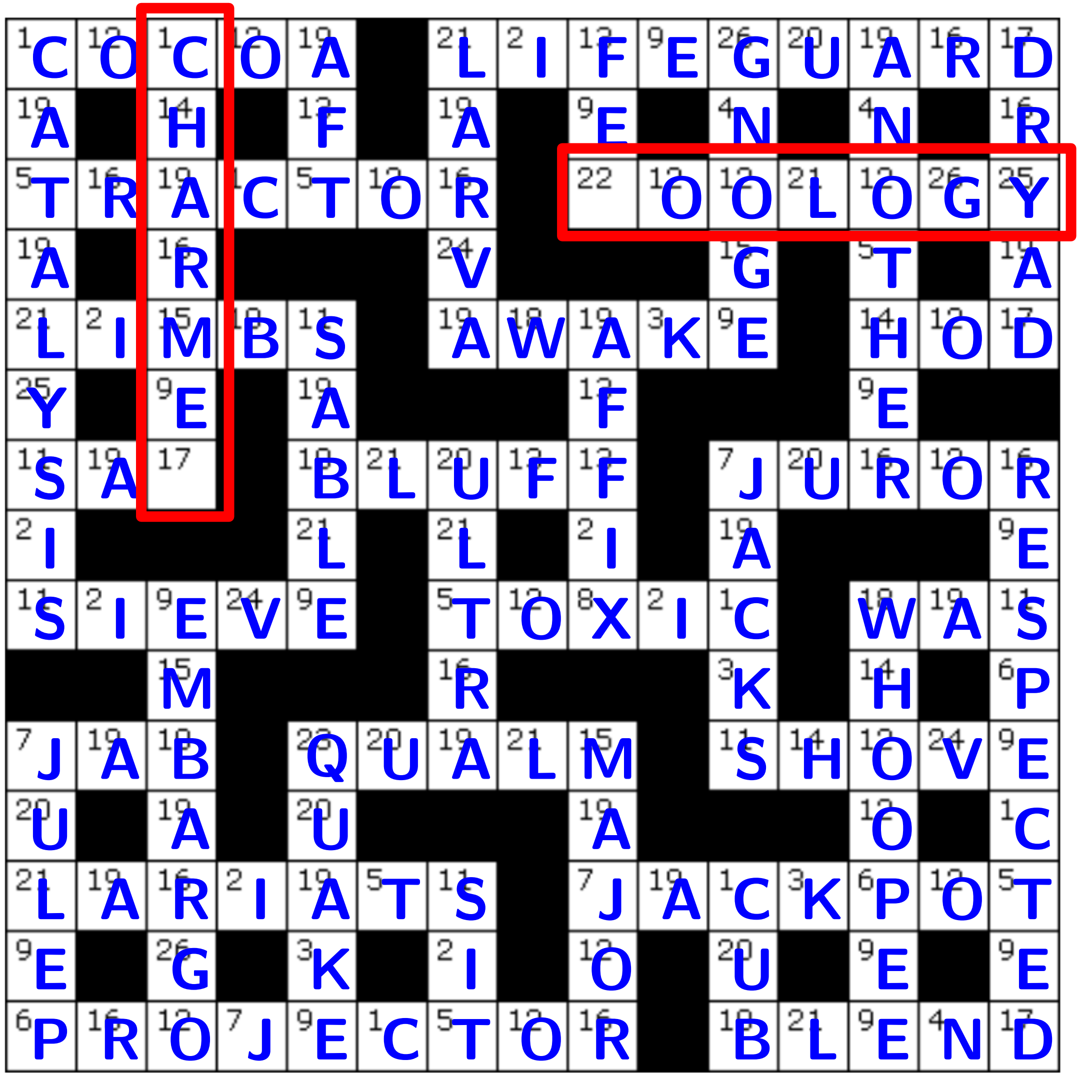
Substitution ciphers



Substitution ciphers

1 C	12 O	1 C	12 O	19 A	■	21 L	2 I	13 F	9 E	26 G	20 U	19 A	16 R	17 D
19 A	■	14 H	■	13 F	■	19 A	■	9 E	■	4 N	■	4 N	■	16 R
5 T	16 R	19 A	1 C	5 T	12 O	16 R	■	22	12 O	12 O	21 L	12 O	26 G	25 Y
19 A	■	16 R	■	■	■	24 V	■	■	■	15 G	■	5 T	■	19 A
21 L	2 I	15 M	10 B	11 S	■	19 A	18 W	19 A	3 K	9 E	■	14 H	12 O	17 D
25 Y	■	9 E	■	19 A	■	■	■	13 F	■	■	■	9 E	■	■
11 S	19 A	17	■	10 B	21 L	20 U	13 F	13 F	■	7 J	20 U	16 R	12 O	16 R
2 I	■	■	■	21 L	■	21 L	■	2 I	■	19 A	■	■	■	9 E
11 S	2 I	9 E	24 V	9 E	■	5 T	12 O	8 X	2 I	1 C	■	18 W	19 A	11 S
■	■	15 M	■	■	■	16 R	■	■	■	3 K	■	14 H	■	6 P
7 J	19 A	10 B	■	23 Q	20 U	19 A	21 L	15 M	■	11 S	14 H	12 O	24 V	9 E
20 U	■	19 A	■	20 U	■	■	■	19 A	■	■	■	12 O	■	1 C
21 L	19 A	16 R	2 I	19 A	5 T	11 S	■	7 J	19 A	1 C	3 K	6 P	12 O	5 T
9 E	■	26 G	■	3 K	■	2 I	■	12 O	■	20 U	■	9 E	■	9 E
6 P	16 R	12 O	7 J	9 E	1 C	5 T	12 O	16 R	■	10 B	21 L	9 E	4 N	17 D

Substitution ciphers



Substitution ciphers

1 C	12 O	1 C	12 O	19 A	■	21 L	2 I	13 F	9 E	26 G	20 U	19 A	16 R	17 D
19 A	■	14 H	■	13 F	■	19 A	■	9 E	■	4 N	■	4 N	■	16 R
5 T	16 R	19 A	1 C	5 T	12 O	16 R	■	22 Z	12 O	12 O	21 L	12 O	26 G	25 Y
19 A	■	16 R	■	■	■	24 V	■	■	■	15 G	■	5 T	■	19 A
21 L	2 I	15 M	10 B	11 S	■	19 A	18 W	19 A	3 K	9 E	■	14 H	12 O	17 D
25 Y	■	9 E	■	19 A	■	■	■	13 F	■	■	■	9 E	■	■
11 S	19 A	17 D	■	10 B	21 L	20 U	13 F	13 F	■	7 J	20 U	16 R	12 O	16 R
2 I	■	■	■	21 L	■	21 L	■	2 I	■	19 A	■	■	■	9 E
11 S	2 I	9 E	24 V	9 E	■	5 T	12 O	8 X	2 I	1 C	■	18 W	19 A	11 S
■	■	15 M	■	■	■	16 R	■	■	■	3 K	■	14 H	■	6 P
7 J	19 A	10 B	■	23 Q	20 U	19 A	21 L	15 M	■	11 S	14 H	12 O	24 V	9 E
20 U	■	19 A	■	20 U	■	■	■	19 A	■	■	■	12 O	■	1 C
21 L	19 A	16 R	2 I	19 A	5 T	11 S	■	7 J	19 A	1 C	3 K	6 P	12 O	5 T
9 E	■	26 G	■	3 K	■	2 I	■	12 O	■	20 U	■	9 E	■	9 E
6 P	16 R	12 O	7 J	9 E	1 C	5 T	12 O	16 R	■	10 B	21 L	9 E	4 N	17 D

Substitution ciphers

How do we decrypt the initial portion of the ciphertext?

Substitution ciphers

How do we decrypt the initial portion of the ciphertext?

We can use a cryptanalysis technique known as *frequency analysis*

Substitution ciphers

How do we decrypt the initial portion of the ciphertext?

We can use a cryptanalysis technique known as *frequency analysis*

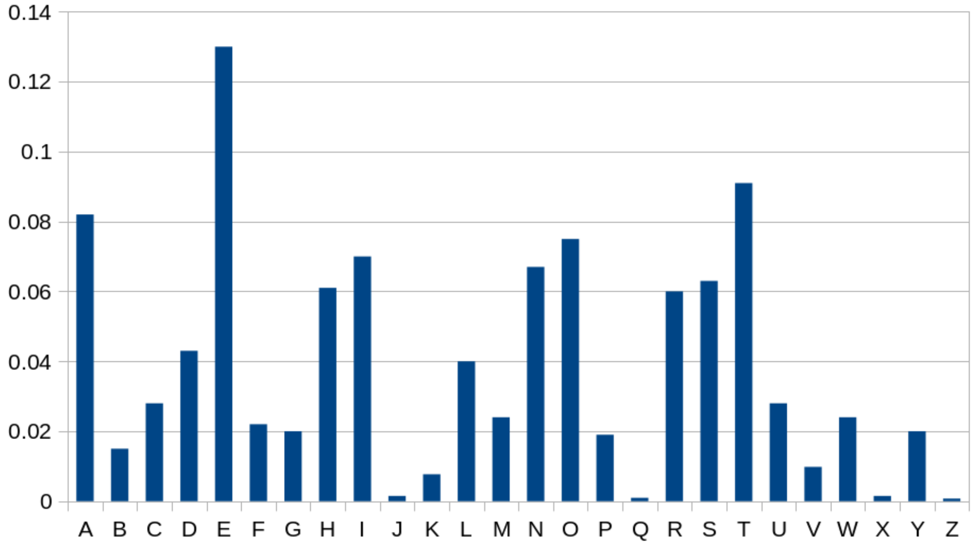
- Natural language has a lot of redundancy
- Messages are far from random
- Different letters appear with different frequencies

Substitution ciphers

How do we decrypt the initial portion of the ciphertext?

We can use a cryptanalysis technique known as *frequency analysis*

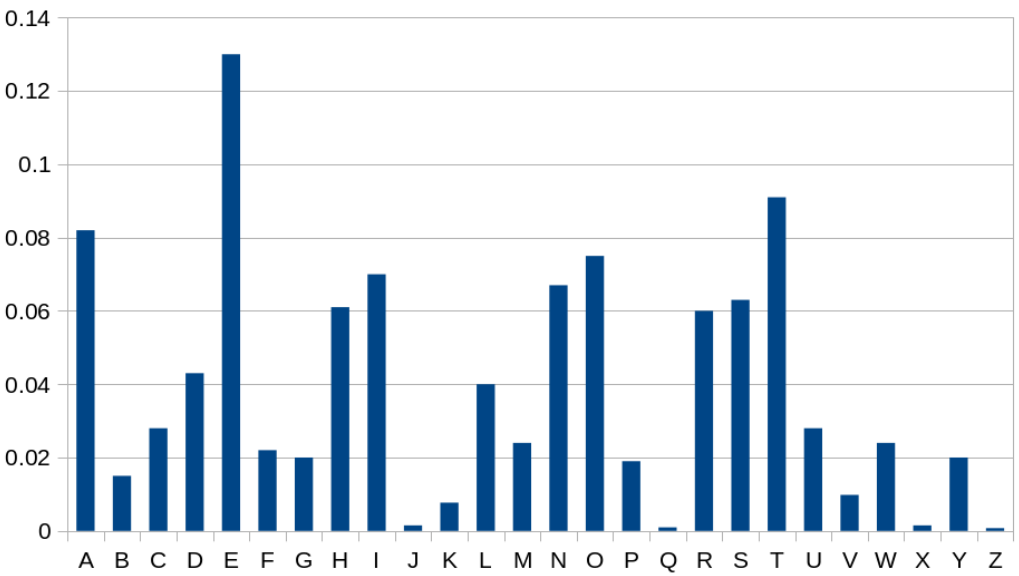
- Natural language has a lot of redundancy
- Messages are far from random
- Different letters appear with different frequencies



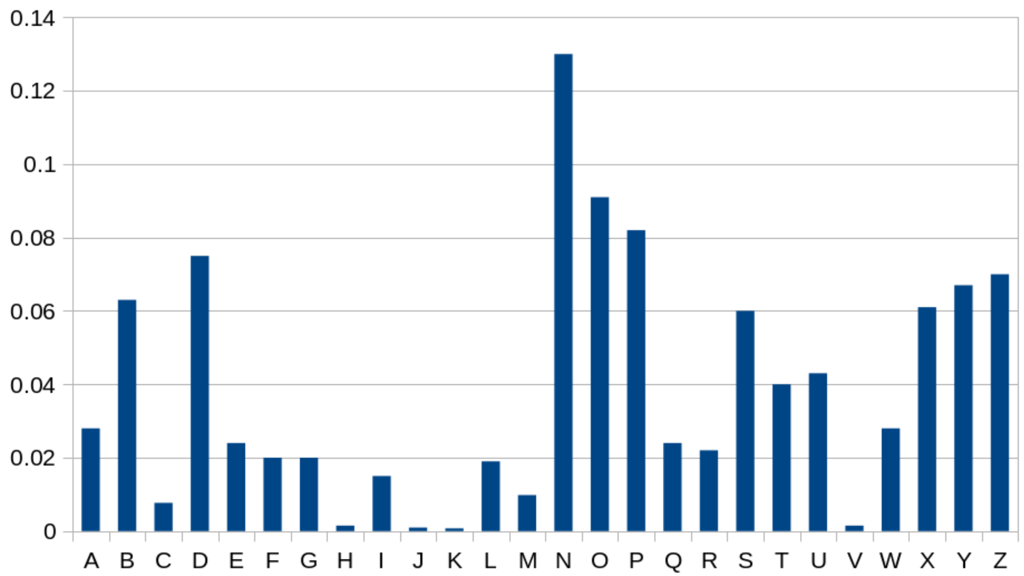
Substitution ciphers

Compare the expected frequencies in the message language with the observed frequencies in the ciphertext

Expected



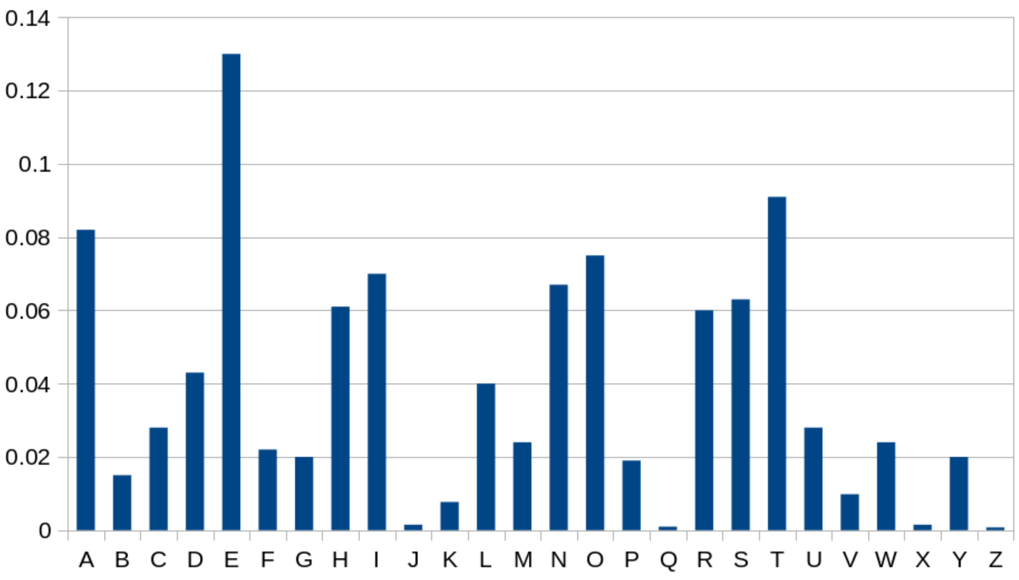
Observed (in the ciphertext)



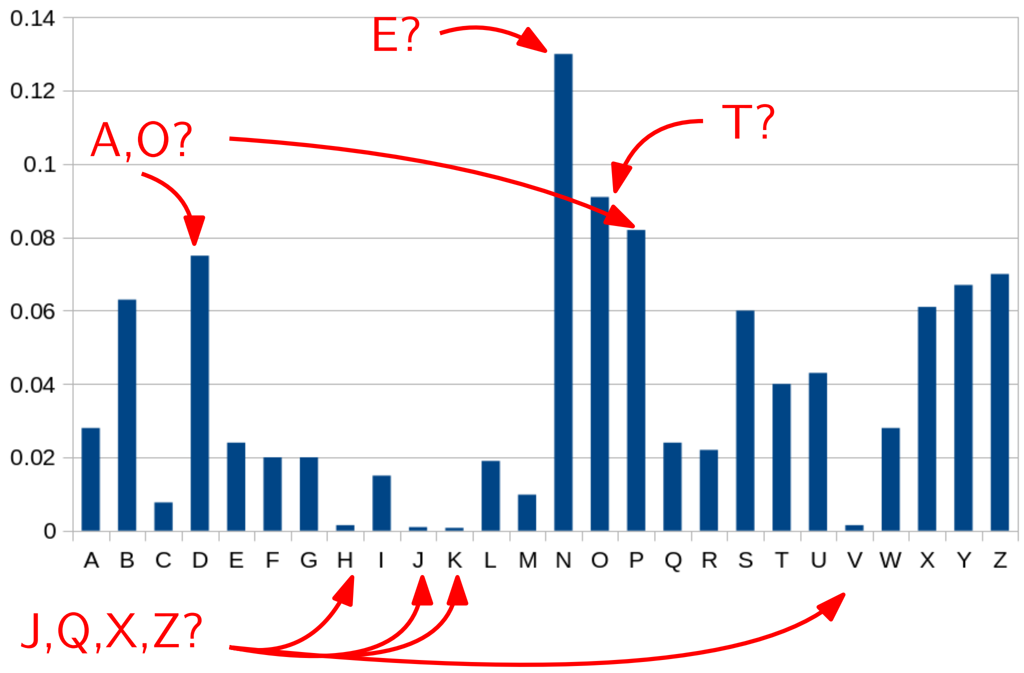
Substitution ciphers

Compare the expected frequencies in the message language with the observed frequencies in the ciphertext

Expected



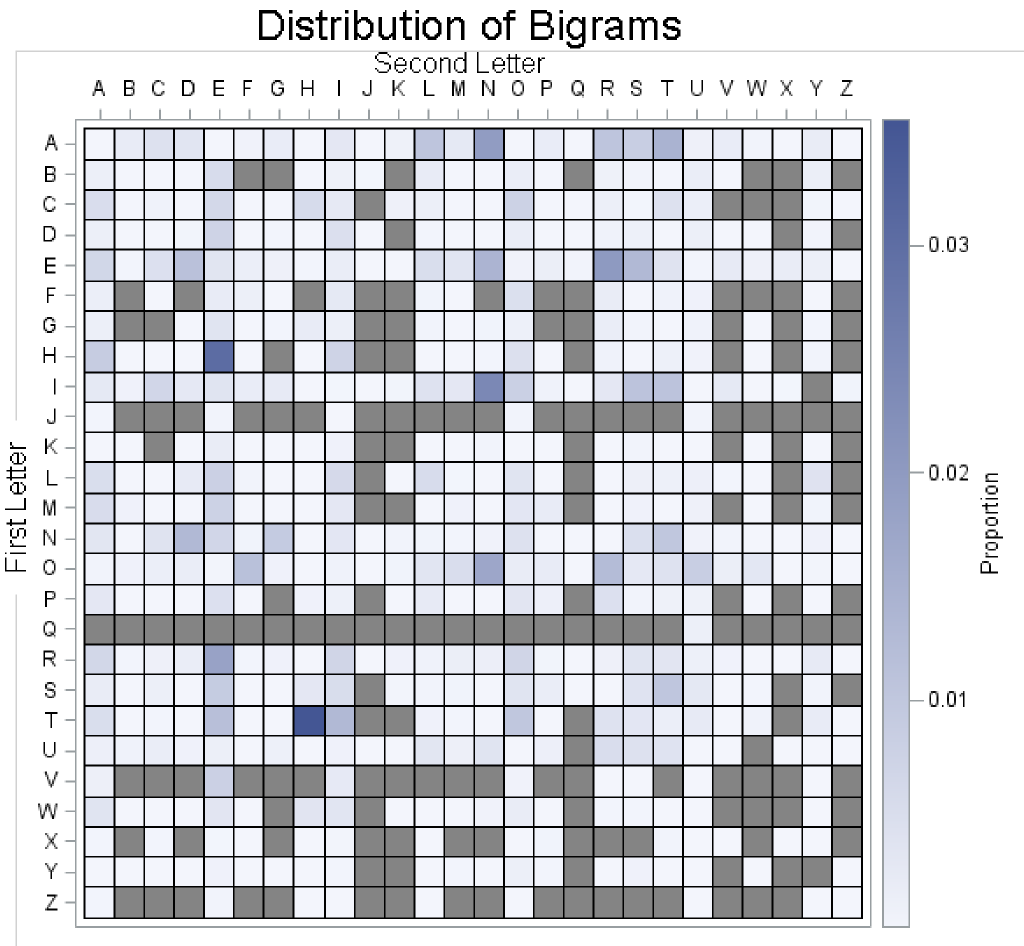
Observed (in the ciphertext)



Guess part of the key and use the guesses to break the cipher (as shown before)

Substitution ciphers

The same analysis can be repeated for bigrams, trigrams, etc



Vigenère cipher

Monoalphabetic substitution ciphers are vulnerable to frequency analysis

Blaise de Vigenère
(1523 - 1596)

Vigenère cipher

Monoalphabetic substitution ciphers are vulnerable to frequency analysis

Idea: mix up the letter frequencies by using different shift ciphers for different positions of the plaintext

Blaise de Vigenère
(1523 - 1596)

Vigenère cipher

Monoalphabetic substitution ciphers are vulnerable to frequency analysis

Idea: mix up the letter frequencies by using different shift ciphers for different positions of the plaintext

The key $k = k_0, k_1, \ldots, k_{t-1}$ is a (non empty) string in $\{A, B, \ldots, Z\}^t$, for some t

Blaise de Vigenère
(1523 - 1596)

Vigenère cipher

Monoalphabetic substitution ciphers are vulnerable to frequency analysis

Idea: mix up the letter frequencies by using different shift ciphers for different positions of the plaintext

The key $k = k_0, k_1, \ldots, k_{t-1}$ is a (non empty) string in $\{A, B, \ldots, Z\}^t$, for some t

The generic i-th character k_i of the key corresponds to the shift $s_i \in \{0, \ldots, 25\}$ of the i-th shift cipher

Blaise de Vigenère
(1523 - 1596)

Vigenère cipher

Monoalphabetic substitution ciphers are vulnerable to frequency analysis

Idea: mix up the letter frequencies by using different shift ciphers for different positions of the plaintext

The key $k = k_0, k_1, \ldots, k_{t-1}$ is a (non empty) string in $\{A, B, \ldots, Z\}^t$, for some t

The generic i-th character k_i of the key corresponds to the shift $s_i \in \{0, \ldots, 25\}$ of the i-th shift cipher

$$s_i = \begin{cases} 0 & \text{if } k_i = \text{A} \\ 1 & \text{if } k_i = \text{B} \\ 2 & \text{if } k_i = \text{C} \\ \ldots & \\ 25 & \text{if } k_i = \text{Z} \end{cases}$$

Blaise de Vigenère
(1523 - 1596)

Vigenère cipher

Monoalphabetic substitution ciphers are vulnerable to frequency analysis

Idea: mix up the letter frequencies by using different shift ciphers for different positions of the plaintext

The key $k = k_0, k_1, \ldots, k_{t-1}$ is a (non empty) string in $\{A, B, \ldots, Z\}^t$, for some t

The generic i-th character k_i of the key corresponds to the shift $s_i \in \{0, \ldots, 25\}$ of the i-th shift cipher

$$s_i = \begin{cases} 0 & \text{if } k_i = \text{A} \\ 1 & \text{if } k_i = \text{B} \\ 2 & \text{if } k_i = \text{C} \\ \ldots & \\ 25 & \text{if } k_i = \text{Z} \end{cases}$$

The generic i-th character m_i of the message $m = m_0 m_1 \ldots m_{\ell-1}$ is encrypted using a shift cipher with shift $s_{i \bmod t}$

Blaise de Vigenère
(1523 - 1596)

Vigenère cipher

$\mathcal{M} = \{A, \ldots, Z\}^*$

$\mathcal{K} = \{A, \ldots, Z\}^t$

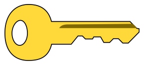
$\mathcal{C} = \{A, \ldots, Z\}^*$

Vigenère cipher

$\mathcal{M} = \{A, \ldots, Z\}^*$

$\mathcal{K} = \{A, \ldots, Z\}^t$

$\mathcal{C} = \{A, \ldots, Z\}^*$

 $k = $ `A C I D`

$m = $ `T H I S N I G H T` $\longrightarrow$ $\boxed{\mathsf{Enc}_k}$

Vigenère cipher

$\mathcal{M} = \{A, \ldots, Z\}^*$

$\mathcal{K} = \{A, \ldots, Z\}^t$

$\mathcal{C} = \{A, \ldots, Z\}^*$

k = `A C I D`

shifts = 0 2 8 3

m = `T H I S N I G H T`

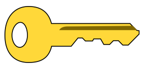
Enc_k

Vigenère cipher

$\mathcal{M} = \{A, \ldots, Z\}^*$

$\mathcal{K} = \{A, \ldots, Z\}^t$

$\mathcal{C} = \{A, \ldots, Z\}^*$

 k = A C I D

shifts = 0 2 8 3

m = T H I S N I G H T

0 2 8 3 0 2 8 3 0

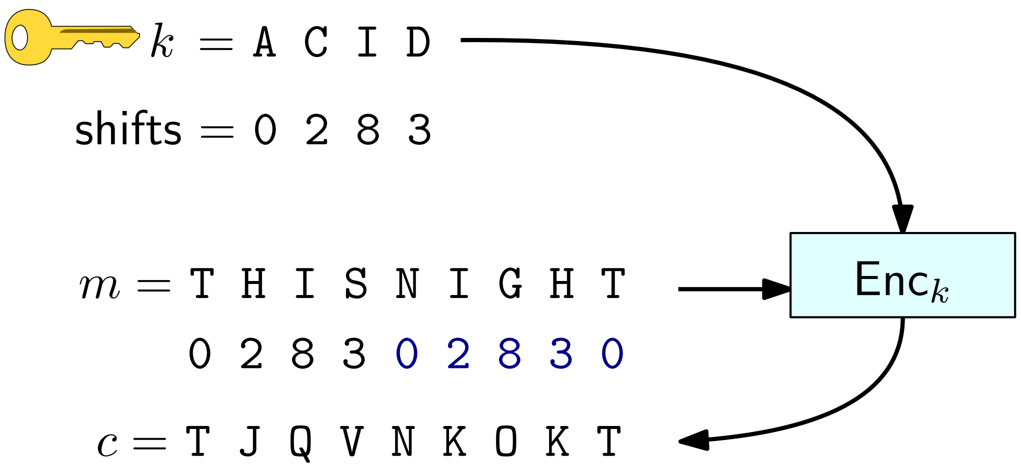
Enc_k

Vigenère cipher

$\mathcal{M} = \{A, \ldots, Z\}^*$

$\mathcal{K} = \{A, \ldots, Z\}^t$

$\mathcal{C} = \{A, \ldots, Z\}^*$

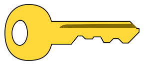


Vigenère cipher

$\mathcal{M} = \{A,\ldots,Z\}^*$

$\mathcal{K} = \{A,\ldots,Z\}^t$

$\mathcal{C} = \{A,\ldots,Z\}^*$

 k = A C I D

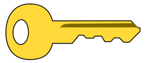
shifts = 0 2 8 3

m = T H I S N I G H T

0 2 8 3 0 2 8 3 0

Enc$_k$

c = T J Q V N K O K T

 k = A C I D

shifts = 0 2 8 3

c = A D Z U T R T D N

Dec$_k$

Vigenère cipher

$\mathcal{M} = \{A, \ldots, Z\}^*$

$\mathcal{K} = \{A, \ldots, Z\}^t$

$\mathcal{C} = \{A, \ldots, Z\}^*$

k = A C I D

shifts = 0 2 8 3

m = T H I S N I G H T

0 2 8 3 0 2 8 3 0

Enc_k

c = T J Q V N K O K T

k = A C I D

shifts = 0 2 8 3

c = A D Z U T R T D N

0 2 8 3 0 2 8 3 0

Dec_k

Vigenère cipher

$\mathcal{M} = \{A, \ldots, Z\}^*$

$\mathcal{K} = \{A, \ldots, Z\}^t$

$\mathcal{C} = \{A, \ldots, Z\}^*$

k = A C I D

shifts = 0 2 8 3

$m =$ T H I S N I G H T $\rightarrow$ $\boxed{\mathsf{Enc}_k}$

0 2 8 3 0 2 8 3 0

$c =$ T J Q V N K O K T

k = A C I D

shifts = 0 2 8 3

$c =$ A D Z U T R T D N $\rightarrow$ $\boxed{\mathsf{Dec}_k}$

0 2 8 3 0 2 8 3 0

$m =$ A B O R T P L A N

Vigenère cipher

A table called “tabula recta” can be used to aid encryption and decryption

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère cipher

A table called "tabula recta" can be used to aid encryption and decryption

E.g., to encrypt the plaintext character `K` with the shift corresponding to the key character `F`, look up the letter at the intersection of the row labeled `K` and the column labeled `F` (or vice-versa)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère cipher

A table called "tabula recta" can be used to aid encryption and decryption

E.g., to encrypt the plaintext character `K` with the shift corresponding to the key character `F`, look up the letter at the intersection of the row labeled `K` and the column labeled `F` (or vice-versa)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère cipher

A table called "tabula recta" can be used to aid encryption and decryption

E.g., to encrypt the plaintext character K with the shift corresponding to the key character F, look up the letter at the intersection of the row labeled K and the column labeled F (or vice-versa)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère cipher

A table called "tabula recta" can be used to aid encryption and decryption

E.g., to encrypt the plaintext character `K` with the shift corresponding to the key character `F`, look up the letter at the intersection of the row labeled `K` and the column labeled `F` (or vice-versa)

To decrypt the ciphertext character `P` with the shift corresponding to the key character `F`, find `P` in the column corresponding to `F` and return the row label

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère cipher

A table called "tabula recta" can be used to aid encryption and decryption

E.g., to encrypt the plaintext character `K` with the shift corresponding to the key character `F`, look up the letter at the intersection of the row labeled `K` and the column labeled `F` (or vice-versa)

To decrypt the ciphertext character `P` with the shift corresponding to the key character `F`, find `P` in the column corresponding to `F` and return the row label

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère cipher

A table called "tabula recta" can be used to aid encryption and decryption

E.g., to encrypt the plaintext character `K` with the shift corresponding to the key character `F`, look up the letter at the intersection of the row labeled `K` and the column labeled `F` (or vice-versa)

To decrypt the ciphertext character `P` with the shift corresponding to the key character `F`, find `P` in the column corresponding to `F` and return the row label

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	$\boxed{P}$	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère cipher

Is Vigenère cipher secure?

Vigenère cipher

Is Vigenère cipher secure? It has been considered secure for centuries...

Vigenère cipher

Is Vigenère cipher secure? It has been considered secure for centuries...

Suppose that the adversary is somehow able to figure out what the length t of the key is

E.g.: $t = 4$

$c =$

```
A M A P A A U H K G O O T W F I O G G G T B T
Q I N N A V S M B T K Q O M O I W C P C T W T
U O I F A G O G T I M O U C F P B T W T B N P
W C P C Q B S J D G F A U O W B O E E K D A E
R K R E M L K B F P R O O T J C C S U O O F S
I Q I W U R B N F W M B T G A A U I E W D F L
Z L S F C Q Z O
```

Vigenère cipher

Is Vigenère cipher secure? It has been considered secure for centuries...

Suppose that the adversary is somehow able to figure out what the length t of the key is

E.g.: $t = 4$

$$
c = \begin{array}{l}
\boxed{\mathtt{A}}\ \mathtt{M\ A\ P}\ \boxed{\mathtt{A}}\ \mathtt{A\ U\ H}\ \boxed{\mathtt{K}}\ \mathtt{G\ O\ O}\ \boxed{\mathtt{T}}\ \mathtt{W\ F\ I}\ \boxed{\mathtt{O}}\ \mathtt{G\ G\ G}\ \boxed{\mathtt{T}}\ \mathtt{B\ T} \\
\mathtt{Q}\ \boxed{\mathtt{I}}\ \mathtt{N\ N\ A}\ \boxed{\mathtt{V}}\ \mathtt{S\ M\ B}\ \boxed{\mathtt{T}}\ \mathtt{K\ Q\ O}\ \boxed{\mathtt{M}}\ \mathtt{O\ I\ W}\ \boxed{\mathtt{C}}\ \mathtt{P\ C\ T}\ \boxed{\mathtt{W}}\ \mathtt{T} \\
\mathtt{U\ O}\ \boxed{\mathtt{I}}\ \mathtt{F\ A\ G}\ \boxed{\mathtt{O}}\ \mathtt{G\ T\ I}\ \boxed{\mathtt{M}}\ \mathtt{O\ U\ C}\ \boxed{\mathtt{F}}\ \mathtt{P\ B\ T}\ \boxed{\mathtt{W}}\ \mathtt{T\ B\ N}\ \boxed{\mathtt{P}} \\
\mathtt{W\ C\ P}\ \boxed{\mathtt{C}}\ \mathtt{Q\ B\ S}\ \boxed{\mathtt{J}}\ \mathtt{D\ G\ F}\ \boxed{\mathtt{A}}\ \mathtt{U\ O\ W}\ \boxed{\mathtt{B}}\ \mathtt{O\ E\ E}\ \boxed{\mathtt{K}}\ \mathtt{D\ A\ E} \\
\boxed{\mathtt{R}}\ \mathtt{K\ R\ E}\ \boxed{\mathtt{M}}\ \mathtt{L\ K\ B}\ \boxed{\mathtt{F}}\ \mathtt{P\ R\ O}\ \boxed{\mathtt{O}}\ \mathtt{T\ J\ C}\ \boxed{\mathtt{C}}\ \mathtt{S\ U\ O}\ \boxed{\mathtt{O}}\ \mathtt{F\ S} \\
\mathtt{I}\ \boxed{\mathtt{Q}}\ \mathtt{I\ W\ U}\ \boxed{\mathtt{R}}\ \mathtt{B\ N\ F}\ \boxed{\mathtt{W}}\ \mathtt{M\ B\ T}\ \boxed{\mathtt{G}}\ \mathtt{A\ A\ U}\ \boxed{\mathtt{I}}\ \mathtt{E\ W\ D}\ \boxed{\mathtt{F}}\ \mathtt{L} \\
\mathtt{Z\ L}\ \boxed{\mathtt{S}}\ \mathtt{F\ C\ Q}\ \boxed{\mathtt{Z}}\ \mathtt{O}
\end{array}
$$

Vigenère cipher

Is Vigenère cipher secure? It has been considered secure for centuries...

Suppose that the adversary is somehow able to figure out what the length t of the key is

E.g.: $t = 4$

$c =$ A M A P A A U H K G O O T W F I O G G G T B T
Q I N N A V S M B T K Q O M O I W C P C T W T
U O I F A G O G T I M O U C F P B T W T B N P
W C P C Q B S J D G F A U O W B O E E K D A E
R K R E M L K B F P R O O T J C C S U O O F S
I Q I W U R B N F W M B T G A A U I E W D F L
Z L S F C Q Z O

Vigenère cipher

Is Vigenère cipher secure? It has been considered secure for centuries...

Suppose that the adversary is somehow able to figure out what the length t of the key is

E.g.: $t = 4$

$c =$ A M A P A A U H K G O O T W F I O G G G T B T
Q I N N A V S M B T K Q O M O I W C P C T W T
U O I F A G O G T I M O U C F P B T W T B N P
W C P C Q B S J D G F A U O W B O E E K D A E
R K R E M L K B F P R O O T J C C S U O O F S
I Q I W U R B N F W M B T G A A U I E W D F L
Z L S F C Q Z O

Vigenère cipher

Is Vigenère cipher secure? It has been considered secure for centuries...

Suppose that the adversary is somehow able to figure out what the length t of the key is

E.g.: $t = 4$

$c =$

A	M	A	P	A	A	U	H	K	G	O	O	T	W	F	I	O	G	G	G	T	B	T
Q	I	N	N	A	V	S	M	B	T	K	Q	O	M	O	I	W	C	P	C	T	W	T
U	O	I	F	A	G	O	G	T	I	M	O	U	C	F	P	B	T	W	T	B	N	P
W	C	P	C	Q	B	S	J	D	G	F	A	U	O	W	B	O	E	E	K	D	A	E
R	K	R	E	M	L	K	B	F	P	R	O	O	T	J	C	C	S	U	O	O	F	S
I	Q	I	W	U	R	B	N	F	W	M	B	T	G	A	A	U	I	E	W	D	F	L
Z	L	S	F	C	Q	Z	O															

The ciphertext can be decomposed into n ciphertext $c^{(1)}, c^{(2)}, \ldots, c^{(t)}$.

Each $c^{(i)}$ is encrypted using the same shift

Each ciphertext can be attacked separately (but we cannot simply bruteforce them)

Breaking the Vigenère cipher

How do we determine the key length?

Breaking the Vigenère cipher

How do we determine the key length?

- **Option 1:** brute-force (guess t and try decrypting the t shift ciphers)

Breaking the Vigenère cipher

How do we determine the key length?

- **Option 1:** brute-force (guess t and try decrypting the t shift ciphers)
- **Option 2:** Kasiski's method

Breaking the Vigenère cipher

How do we determine the key length?

- **Option 1:** brute-force (guess t and try decrypting the t shift ciphers)
- **Option 2:** Kasiski's method
- **Option 3:** Index of coincidence method

Breaking the Vigenère cipher

How do we determine the key length?

- **Option 1:** brute-force (guess t and try decrypting the t shift ciphers)
- **Option 2:** Kasiski's method
- **Option 3:** Index of coincidence method

Kasiski's method

- Consider some (unknown) sequence of characters that appears frequently in the plaintext (for example the word "the")

```
T H E M A N A N D T H E W O M A N R E T R I E V E D T H E L E T T E R F R O M T H E P O S T B O X
B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D
-------------------------------------------------------------------------------------------------
U L E P S O E N G L I I W R E B R R H L S M E Y W E X H H D F X T H J G V O P L I I P R K U F O A
```

Kasiski's method

- Consider some (unknown) sequence of characters that appears frequently in the plaintext (for example the word "the")

T H E M A N A N D T H E W O M A N R E T R I E V E D T H E L E T T E R F R O M T H E P O S T B O X

B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D

U L E P S O E N G L I I W R E B R R H L S M E Y W E X H H D F X T H J G V O P L I I P R K U F O A

Kasiski's method

- Consider some (unknown) sequence of characters that appears frequently in the plaintext (for example the word "the")
- In general, distinct occurrences of the word will be encrypted using different portions of the key and the ciphertext characters will differ

```
[T H E] M A N A N D [T H E] W O M A N R E T R I E V E D [T H E] L E T T E R F R O M [T H E] P O S T B O X
 B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D
-----------------------------------------------------------------------------------------------------
[U L E] P S O E N G L I I W R E B R R H L S M E Y W E [X H H] D F X T H J G V O P L I I P R K U F O A
```

Kasiski's method

- Consider some (unknown) sequence of characters that appears frequently in the plaintext (for example the word "the")
- In general, distinct occurrences of the word will be encrypted using different portions of the key and the ciphertext characters will differ
- However, some occurrences will happen to *line up* (i.e., be encrypted with the same portion of the key)

```
T H E M A N A N D T H E W O M A N R E T R I E V E D T H E L E T T E R F R O M T H E P O S T B O X
B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D
-------------------------------------------------------------------------------------------------
U L E P S O E N G L I I W R E B R R H L S M E Y W E X H H D F X T H J G V O P L I I P R K U F O A
```

Kasiski's method

- Consider some (unknown) sequence of characters that appears frequently in the plaintext (for example the word "the")

- In general, distinct occurrences of the word will be encrypted using different portions of the key and the ciphertext characters will differ

- However, some occurrences will happen to *line up* (i.e., be encrypted with the same portion of the key)

- When this happens, the corresponding portions of ciphertext will be equal

```
T H E M A N A N D T H E W O M A N R E T R I E V E D T H E L E T T E R F R O M T H E P O S T B O X
B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D
-------------------------------------------------------------------------------------------------
U L E P S O E N G L I I W R E B R R H L S M E Y W E X H H D F X T H J G V O P L I I P R K U F O A
```

Kasiski's method

```
T H E M A N A N D T H E W O M A N R E T R I E V E D T H E L E T T E R F R O M T H E P O S T B O X
B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D
-------------------------------------------------------------------------------------------------
U L E P S O E N G L I I W R E B R R H L S M E Y W E X H H D F X T H J G V O P L I I P R K U F O A
```

distance $= 30$

Obs: The distance between repeated patterns in the ciphertext is likely to be a multiple of the key length

Kasiski's method

```
T H E M A N A N D T H E W O M A N R E T R I E V E D T H E L E T T E R F R O M T H E P O S T B O X
B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D
-------------------------------------------------------------------------------------------------
U L E P S O E N G L I I W R E B R R H L S M E Y W E X H H D F X T H J G V O P L I I P R K U F O A
```

distance $= 30$

Obs: The distance between repeated patterns in the ciphertext is likely to be a multiple of the key length

- Find some repeated patterns of small length (e.g., 2 or 3) in the ciphertext

Kasiski's method

T H E M A N A N D T H E W O M A N R E T R I E V E D T H E L E T T E R F R O M T H E P O S T B O X

B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D

U L E P S O E N G L I I W R E B R R H L S M E Y W E X H H D F X T H J G V O P L I I P R K U F O A

distance $= 30$

Obs: The distance between repeated patterns in the ciphertext is likely to be a multiple of the key length

- Find some repeated patterns of small length (e.g., 2 or 3) in the ciphertext
- Look at the distances between pairs of repetitions

Kasiski's method

```
T H E M A N A N D T H E W O M A N R E T R I E V E D T H E L E T T E R F R O M T H E P O S T B O X
B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D
-------------------------------------------------------------------------------------------------
U L E P S O E N G L I I W R E B R R H L S M E Y W E X H H D F X T H J G V O P L I I P R K U F O A
```

distance $= 30$

Obs: The distance between repeated patterns in the ciphertext is likely to be a multiple of the key length

- Find some repeated patterns of small length (e.g., 2 or 3) in the ciphertext
- Look at the distances between pairs of repetitions
- Use the greatest common divisor among the distances as a guess for the key length t

Kasiski's method

```
T H E M A N A N D T H E W O M A N R E T R I E V E D T H E L E T T E R F R O M T H E P O S T B O X
B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D S B E A D
-------------------------------------------------------------------------------------------------
U L E P S O E N G L I I W R E B R R H L S M E Y W E X H H D F X T H J G V O P L I I P R K U F O A
```

distance $= 30$

Obs: The distance between repeated patterns in the ciphertext is likely to be a multiple of the key length

- Find some repeated patterns of small length (e.g., 2 or 3) in the ciphertext
- Look at the distances between pairs of repetitions
- Use the greatest common divisor among the distances as a guess for the key length t

In the example the key length t is 5 and the distance between patterns is 30

Breaking the Vigenère cipher

How do we determine the key length?

- **Option 1:** brute-force (guess n and try decrypting the n shift ciphers)
- **Option 2:** Kasiski's method
- **Option 3:** Index of coincidence method

Index of coincidence method

Let p_j be the expected frequency of the j-th letter $(j = 0. \dots, 25)$ in the language of the plaintext

Using the frequencies in the English language: $$\sum_{j=0}^{25} p_j^2 \approx 0.065$$

Index of coincidence method

Let p_j be the expected frequency of the j-th letter $(j = 0. \ldots, 25)$ in the language of the plaintext

Using the frequencies in the English language: $$\sum_{j=0}^{25} p_j^2 \approx 0.065$$

Guess that the key length is τ and split the ciphertext into $c^{(1)}, \ldots, c^{(\tau)}$ sub-ciphertexts (as before).
For a given i, let q_j be the observed frequency of the j-th letter of the alphabet in $c^{(i)}$.

Compute $$S_\tau = \sum_{i=0}^{25} q_j^2$$

Index of coincidence method

Let p_j be the expected frequency of the j-th letter $(j = 0. \dots, 25)$ in the language of the plaintext

Using the frequencies in the English language: $$\sum_{j=0}^{25} p_j^2 \approx 0.065$$

Guess that the key length is τ and split the ciphertext into $c^{(1)}, \dots, c^{(\tau)}$ sub-ciphertexts (as before).
For a given i, let q_j be the observed frequency of the j-th letter of the alphabet in $c^{(i)}$.

Compute $S_\tau = \sum_{i=0}^{25} q_j^2$

If τ is a multiple of the actual key length t, all the symbols of $c^{(i)}$ are encrypted with a fixed shift

Index of coincidence method

Let p_j be the expected frequency of the j-th letter $(j = 0. \dots, 25)$ in the language of the plaintext

Using the frequencies in the English language: $$\sum_{j=0}^{25} p_j^2 \approx 0.065$$

Guess that the key length is τ and split the ciphertext into $c^{(1)}, \dots, c^{(\tau)}$ sub-ciphertexts (as before).
For a given i, let q_j be the observed frequency of the j-th letter of the alphabet in $c^{(i)}$.

Compute $S_\tau = \sum_{i=0}^{25} q_j^2$

If τ is a multiple of the actual key length t, all the symbols of $c^{(i)}$ are encrypted with a fixed shift

$\implies$ their frequencies q_j resemble p_j, up to some shift

Index of coincidence method

Let p_j be the expected frequency of the j-th letter $(j = 0. \dots, 25)$ in the language of the plaintext

Using the frequencies in the English language: $$\sum_{j=0}^{25} p_j^2 \approx 0.065$$

Guess that the key length is τ and split the ciphertext into $c^{(1)}, \dots, c^{(\tau)}$ sub-ciphertexts (as before).
For a given i, let q_j be the observed frequency of the j-th letter of the alphabet in $c^{(i)}$.

Compute $$S_\tau = \sum_{i=0}^{25} q_j^2$$

If τ is a multiple of the actual key length t, all the symbols of $c^{(i)}$ are encrypted with a fixed shift

$\Longrightarrow$ their frequencies q_j resemble p_j, up to some shift $\Longrightarrow$ $S_\tau = \sum_{j=0}^{25} q_j^2 \approx \sum_{j=0}^{25} p_j^2 \approx 0.065$

Index of coincidence method

Let p_j be the expected frequency of the j-th letter $(j = 0. \dots, 25)$ in the language of the plaintext

Using the frequencies in the English language: $$\sum_{j=0}^{25} p_j^2 \approx 0.065$$

Guess that the key length is τ and split the ciphertext into $c^{(1)}, \dots, c^{(\tau)}$ sub-ciphertexts (as before).
For a given i, let q_j be the observed frequency of the j-th letter of the alphabet in $c^{(i)}$.

Compute $$S_\tau = \sum_{i=0}^{25} q_j^2$$

If τ is a multiple of the actual key length t, all the symbols of $c^{(i)}$ are encrypted with a fixed shift

$\implies$ their frequencies q_j resemble p_j, up to some shift $\implies S_\tau = \sum_{j=0}^{25} q_j^2 \approx \sum_{j=0}^{25} p_j^2 \approx 0.065$

If τ is not a multiple of t, then we expect that all characters in $c^{(i)}$ will occur with equal probability

Index of coincidence method

Let p_j be the expected frequency of the j-th letter ($j = 0. \dots, 25$) in the language of the plaintext

Using the frequencies in the English language: $$\sum_{j=0}^{25} p_j^2 \approx 0.065$$

Guess that the key length is τ and split the ciphertext into $c^{(1)}, \dots, c^{(\tau)}$ sub-ciphertexts (as before).
For a given i, let q_j be the observed frequency of the j-th letter of the alphabet in $c^{(i)}$.

Compute $$S_\tau = \sum_{i=0}^{25} q_j^2$$

If τ is a multiple of the actual key length t, all the symbols of $c^{(i)}$ are encrypted with a fixed shift

$\implies$ their frequencies q_j resemble p_j, up to some shift $\implies S_\tau = \sum_{j=0}^{25} q_j^2 \approx \sum_{j=0}^{25} p_j^2 \approx 0.065$

If τ is not a multiple of t, then we expect that all characters in $c^{(i)}$ will occur with equal probability

$\implies S_\tau \approx \sum_{j=0}^{25} \left(\frac{1}{26}\right)^2 \approx 0.038$

Index of coincidence method

Let p_j be the expected frequency of the j-th letter ($j = 0. \ldots, 25$) in the language of the plaintext

Using the frequencies in the English language: $$\sum_{j=0}^{25} p_j^2 \approx 0.065$$

Guess that the key length is τ and split the ciphertext into $c^{(1)}, \ldots, c^{(\tau)}$ sub-ciphertexts (as before).
For a given i, let q_j be the observed frequency of the j-th letter of the alphabet in $c^{(i)}$.

Compute $$S_\tau = \sum_{i=0}^{25} q_j^2$$

The smallest value of τ such that $S_\tau \approx 0.065$ is probably the length of the key

This can be validated by repeating the check for other values of i

Breaking the Vigenère cipher

How do we break the shift ciphers?

- We will show an attack that requires the letters to follow the frequencies of a natural language...

Breaking the Vigenère cipher

How do we break the shift ciphers?

- We will show an attack that requires the letters to follow the frequencies of a natural language...
- ... but we do not need the message to make sense!

(In particular, it can be applied to the shift ciphers obtained by decomposing the ciphertext of the Vigenère cipher)

Breaking the Vigenère cipher

How do we break the shift ciphers?

- We will show an attack that requires the letters to follow the frequencies of a natural language...
- ... but we do not need the message to make sense!

  (In particular, it can be applied to the shift ciphers obtained by decomposing the ciphertext of the Vigenère cipher)

Guess the shift j of the cipher:

- If the guess is correct then the i-th letter in the alphabet is mapped to the $(i + j)$-th letter $\pmod{26}$

Breaking the Vigenère cipher

How do we break the shift ciphers?

- We will show an attack that requires the letters to follow the frequencies of a natural language...
- ... but we do not need the message to make sense!

  (In particular, it can be applied to the shift ciphers obtained by decomposing the ciphertext of the Vigenère cipher)

Guess the shift j of the cipher:

- If the guess is correct then the i-th letter in the alphabet is mapped to the $(i+j)$-th letter $\pmod{26}$

  We expect: $q_{(i+j) \bmod 26} \approx p_i$

Breaking the Vigenère cipher

How do we break the shift ciphers?

- We will show an attack that requires the letters to follow the frequencies of a natural language...
- ... but we do not need the message to make sense!

  (In particular, it can be applied to the shift ciphers obtained by decomposing the ciphertext of the Vigenère cipher)

Guess the shift j of the cipher:

- If the guess is correct then the i-th letter in the alphabet is mapped to the $(i+j)$-th letter $\pmod{26}$

  We expect: $q_{(i+j) \bmod 26} \approx p_i \implies \sum_{i=0}^{25} p_i q_{(i+j) \bmod 26} \approx \sum_{i=0}^{25} p_i^2 \approx 0.065$

Breaking the Vigenère cipher

How do we break the shift ciphers?

- We will show an attack that requires the letters to follow the frequencies of a natural language...
- ... but we do not need the message to make sense!

  (In particular, it can be applied to the shift ciphers obtained by decomposing the ciphertext of the Vigenère cipher)

Guess the shift j of the cipher:

- If the guess is correct then the i-th letter in the alphabet is mapped to the $(i + j)$-th letter $\pmod{26}$

  We expect: $q_{(i+j) \bmod 26} \approx p_i \implies \sum_{i=0}^{25} p_i q_{(i+j) \bmod 26} \approx \sum_{i=0}^{25} p_i^2 \approx 0.065$

- If the guess is wrong, we expect $\sum_{i=0}^{25} p_i q_{(i+j) \bmod 26}$ to be "far enough" from 0.065

Breaking the Vigenère cipher

How do we break the shift ciphers?

- We will show an attack that requires the letters to follow the frequencies of a natural language...
- ... but we do not need the message to make sense!

(In particular, it can be applied to the shift ciphers obtained by decomposing the ciphertext of the Vigenère cipher)

Guess the shift j of the cipher:

- If the guess is correct then the i-th letter in the alphabet is mapped to the $(i+j)$-th letter $\pmod{26}$

  We expect: $q_{(i+j) \bmod 26} \approx p_i \quad \Longrightarrow \sum_{i=0}^{25} p_i q_{(i+j) \bmod 26} \approx \sum_{i=0}^{25} p_i^2 \approx 0.065$

- If the guess is wrong, we expect $\sum_{i=0}^{25} p_i q_{(i+j) \bmod 26}$ to be "far enough" from 0.065

Compute $I_j = \sum_{i=0}^{25} p_i q_{(i+j)} \bmod 26$ for all possible shifts j and choose the one for which I_j is closest to 0.065.

A famous polyalphabetic substitution cipher

The Vigenère cipher is a particular polyalphabetic substituion cipher (different positions in the plaintext are encrypted using different "alphabets")

A famous polyalphabetic substitution cipher

The Vigenère cipher is a particular polyalphabetic substituion cipher (different positions in the plaintext are encrypted using different "alphabets")

Another famous polyalphabetic substitution cipher:

A famous polyalphabetic substitution cipher

The Vigenère cipher is a particular polyalphabetic substituion cipher (different positions in the plaintext are encrypted using different "alphabets")

Another famous polyalphabetic substitution cipher:

Marian Adam Rejewski

Alan Mathison Turing

Scytale cipher

A way used to encrypt a message using a rod (the scytale, or skytale) and a strip of parchment

Scytale cipher

A way used to encrypt a message using a rod (the scytale, or skytale) and a strip of parchment

The parchment is wound around the rod, and the plaintext is written along the length of the rod

Scytale cipher

A way used to encrypt a message using a rod (the scytale, or skytale) and a strip of parchment

The parchment is wound around the rod, and the plaintext is written along the length of the rod

The ciphertext consists of the unwound stip of parchment (without the rod)

Scytale cipher

A way used to encrypt a message using a rod (the scytale, or skytale) and a strip of parchment

The parchment is wound around the rod, and the plaintext is written along the length of the rod

The ciphertext consists of the unwound stip of parchment (without the rod)

This cipher is said to have been used by the ancient greeks to communicate during the military campaigns

Scytale cipher

A way used to encrypt a message using a rod (the scytale, or skytale) and a strip of parchment

The parchment is wound around the rod, and the plaintext is written along the length of the rod

The ciphertext consists of the unwound stip of parchment (without the rod)

This cipher is said to have been used by the ancient greeks to communicate during the military campaigns

What is the key of this cipher?

Scytale cipher

A way used to encrypt a message using a rod (the scytale, or skytale) and a strip of parchment

The parchment is wound around the rod, and the plaintext is written along the length of the rod

The ciphertext consists of the unwound stip of parchment (without the rod)

This cipher is said to have been used by the ancient greeks to communicate during the military campaigns

What is the key of this cipher? The diameter of the rod!

Scytale cipher

A way used to encrypt a message using a rod (the scytale, or skytale) and a strip of parchment

The parchment is wound around the rod, and the plaintext is written along the length of the rod

The ciphertext consists of the unwound stip of parchment (without the rod)

This cipher is said to have been used by the ancient greeks to communicate during the military campaigns

What is the key of this cipher? The diameter of the rod!

To decrypt the ciphertext, simply wind it around a rod of the same diameter

Breaking the scytale cipher

Breaking the scytale cipher

Wind the parchment around a cone

Look for the portion of the cone where letters start to line up and produce sensible words

The corresponding diameter is the key!

Scytale cipher

What is the effect of winding the parchment around the scytale on the order of the characters in the plaintext?

Scytale cipher

What is the effect of winding the parchment around the scytale on the order of the characters in the plaintext?

$m =$ K I L L K I N G T O M O R R O W M I D N I G H T

$c =$ K T M I O I L M D L O N K R I I R G N O H G W T

Scytale cipher

What is the effect of winding the parchment around the scytale on the order of the characters in the plaintext?

$m =$ `K I L L K I N G T O M O R R O W M I D N I G H T`

$c =$ `K T M I O I L M D L O N K R I I R G N O H G W T`


```
      K I L L K I N G
m =   T O M O R R O W
      M I D N I G H T
```

Scytale cipher

What is the effect of winding the parchment around the scytale on the order of the characters in the plaintext?

$m =$ K I L L K I N G T O M O R R O W M I D N I G H T

$c =$ K T M I O I L M D L O N K R I I R G N O H G W T

$$m = \begin{bmatrix} \mathtt{K} & \mathtt{I} & \mathtt{L} & \mathtt{L} & \mathtt{K} & \mathtt{I} & \mathtt{N} & \mathtt{G} \\ \mathtt{T} & \mathtt{O} & \mathtt{M} & \mathtt{O} & \mathtt{R} & \mathtt{R} & \mathtt{O} & \mathtt{W} \\ \mathtt{M} & \mathtt{I} & \mathtt{D} & \mathtt{N} & \mathtt{I} & \mathtt{G} & \mathtt{H} & \mathtt{T} \end{bmatrix}$$

Scytale cipher

What is the effect of winding the parchment around the scytale on the order of the characters in the plaintext?

$m = \mathtt{K\ I\ L\ L\ K\ I\ N\ G\ T\ O\ M\ O\ R\ R\ O\ W\ M\ I\ D\ N\ I\ G\ H\ T}$

$c = \mathtt{K\ T\ M\ I\ O\ I\ L\ M\ D\ L\ O\ N\ K\ R\ I\ I\ R\ G\ N\ O\ H\ G\ W\ T}$

$$\begin{bmatrix} \mathtt{K} & \mathtt{I} & \mathtt{L} & \mathtt{L} & \mathtt{K} & \mathtt{I} & \mathtt{N} & \mathtt{G} \\ \mathtt{T} & \mathtt{O} & \mathtt{M} & \mathtt{O} & \mathtt{R} & \mathtt{R} & \mathtt{O} & \mathtt{W} \\ \mathtt{M} & \mathtt{I} & \mathtt{D} & \mathtt{N} & \mathtt{I} & \mathtt{G} & \mathtt{H} & \mathtt{T} \end{bmatrix}^{\mathsf{T}}$$

Scytale cipher

What is the effect of winding the parchment around the scytale on the order of the characters in the plaintext?

$m =$ K I L L K I N G T O M O R R O W M I D N I G H T

$c =$ K T M I O I L M D L O N K R I I R G N O H G W T

$$\begin{bmatrix} \mathtt{K} & \mathtt{I} & \mathtt{L} & \mathtt{L} & \mathtt{K} & \mathtt{I} & \mathtt{N} & \mathtt{G} \\ \mathtt{T} & \mathtt{O} & \mathtt{M} & \mathtt{O} & \mathtt{R} & \mathtt{R} & \mathtt{O} & \mathtt{W} \\ \mathtt{M} & \mathtt{I} & \mathtt{D} & \mathtt{N} & \mathtt{I} & \mathtt{G} & \mathtt{H} & \mathtt{T} \end{bmatrix}^{\mathsf{T}} = \begin{bmatrix} \mathtt{K} & \mathtt{T} & \mathtt{M} \\ \mathtt{I} & \mathtt{O} & \mathtt{I} \\ \mathtt{L} & \mathtt{M} & \mathtt{D} \\ \mathtt{L} & \mathtt{O} & \mathtt{N} \\ \mathtt{K} & \mathtt{R} & \mathtt{I} \\ \mathtt{I} & \mathtt{R} & \mathtt{G} \\ \mathtt{N} & \mathtt{O} & \mathtt{H} \\ \mathtt{G} & \mathtt{W} & \mathtt{T} \end{bmatrix}$$

Scytale cipher

What is the effect of winding the parchment around the scytale on the order of the characters in the plaintext?

$$m = \texttt{K I L L K I N G T O M O R R O W M I D N I G H T}$$

$$c = \texttt{K T M I O I L M D L O N K R I I R G N O H G W T}$$

$$\begin{bmatrix} \texttt{K} & \texttt{I} & \texttt{L} & \texttt{L} & \texttt{K} & \texttt{I} & \texttt{N} & \texttt{G} \\ \texttt{T} & \texttt{O} & \texttt{M} & \texttt{O} & \texttt{R} & \texttt{R} & \texttt{O} & \texttt{W} \\ \texttt{M} & \texttt{I} & \texttt{D} & \texttt{N} & \texttt{I} & \texttt{G} & \texttt{H} & \texttt{T} \end{bmatrix}^{\mathsf{T}} = \begin{bmatrix} \texttt{K} & \texttt{T} & \texttt{M} \\ \texttt{I} & \texttt{O} & \texttt{I} \\ \texttt{L} & \texttt{M} & \texttt{D} \\ \texttt{L} & \texttt{O} & \texttt{N} \\ \texttt{K} & \texttt{R} & \texttt{I} \\ \texttt{I} & \texttt{R} & \texttt{G} \\ \texttt{N} & \texttt{O} & \texttt{H} \\ \texttt{G} & \texttt{W} & \texttt{T} \end{bmatrix} = c$$

Scytale cipher

What is the effect of winding the parchment around the scytale on the order of the characters in the plaintext?

$m = \mathtt{K\ I\ L\ L\ K\ I\ N\ G\ T\ O\ M\ O\ R\ R\ O\ W\ M\ I\ D\ N\ I\ G\ H\ T}$

$c = \mathtt{K\ T\ M\ I\ O\ I\ L\ M\ D\ L\ O\ N\ K\ R\ I\ I\ R\ G\ N\ O\ H\ G\ W\ T}$

$$\begin{bmatrix} \mathtt{K} & \mathtt{I} & \mathtt{L} & \mathtt{L} & \mathtt{K} & \mathtt{I} & \mathtt{N} & \mathtt{G} \\ \mathtt{T} & \mathtt{O} & \mathtt{M} & \mathtt{O} & \mathtt{R} & \mathtt{R} & \mathtt{O} & \mathtt{W} \\ \mathtt{M} & \mathtt{I} & \mathtt{D} & \mathtt{N} & \mathtt{I} & \mathtt{G} & \mathtt{H} & \mathtt{T} \end{bmatrix}^{\mathsf{T}} = \begin{bmatrix} \mathtt{K} & \mathtt{T} & \mathtt{M} \\ \mathtt{I} & \mathtt{O} & \mathtt{I} \\ \mathtt{L} & \mathtt{M} & \mathtt{D} \\ \mathtt{L} & \mathtt{O} & \mathtt{N} \\ \mathtt{K} & \mathtt{R} & \mathtt{I} \\ \mathtt{I} & \mathtt{R} & \mathtt{G} \\ \mathtt{N} & \mathtt{O} & \mathtt{H} \\ \mathtt{G} & \mathtt{W} & \mathtt{T} \end{bmatrix} = c$$

The scytale cipher is a (specific type of) transposition cipher!

(Columnar) Transposition ciphers

The plaintext is arranged in a matrix with n columns (and the appropriate number of rows)

(Columnar) Transposition ciphers

The plaintext is arranged in a matrix with n columns (and the appropriate number of rows)

1	2	3	4	5	6
T	H	E	M	E	E
T	I	N	G	I	S
T	O	M	O	R	R
O	W	A	T	T	H
E	D	O	C	K	

(Columnar) Transposition ciphers

The plaintext is arranged in a matrix with n columns (and the appropriate number of rows)

1	2	3	4	5	6
T	H	E	M	E	E
T	I	N	G	I	S
T	O	M	O	R	R
O	W	A	T	T	H
E	D	O	C	K	$\boxed{\texttt{X}}$

The message might or might not be padded with random characters (`X` in this case) to fill the last row.

(Columnar) Transposition ciphers

The plaintext is arranged in a matrix with n columns (and the appropriate number of rows)

1	2	3	4	5	6
T	H	E	M	E	E
T	I	N	G	I	S
T	O	M	O	R	R
O	W	A	T	T	H
E	D	O	C	K	$\boxed{X}$

The message might or might not be padded with random characters (X in this case) to fill the last row.

Regular vs. Irregular transposition ciphers

(Columnar) Transposition ciphers

The plaintext is arranged in a matrix with n columns (and the appropriate number of rows)

1	2	3	4	5	6
T	H	E	M	E	E
T	I	N	G	I	S
T	O	M	O	R	R
O	W	A	T	T	H
E	D	O	C	K	$\boxed{\texttt{X}}$

The message might or might not be padded with random characters (`X` in this case) to fill the last row.

Regular vs. Irregular transposition ciphers

Pick a permutation π of $1, 2, \ldots, n$

(Columnar) Transposition ciphers

The plaintext is arranged in a matrix with n columns (and the appropriate number of rows)

1	2	3	4	5	6
T	H	E	M	E	E
T	I	N	G	I	S
T	O	M	O	R	R
O	W	A	T	T	H
E	D	O	C	K	$\boxed{\texttt{X}}$

The message might or might not be padded with random characters (`X` in this case) to fill the last row.

Regular vs. Irregular transposition ciphers

Pick a permutation π of $1, 2, \ldots, n$

The ciphertext is obtained by reading the columns from top to bottom, in the order given by π

(Columnar) Transposition ciphers

The plaintext is arranged in a matrix with n columns (and the appropriate number of rows)

1	2	3	4	5	6
T	H	E	M	E	E
T	I	N	G	I	S
T	O	M	O	R	R
O	W	A	T	T	H
E	D	O	C	K	X

The message might or might not be padded with random characters (X in this case) to fill the last row.

Regular vs. Irregular transposition ciphers

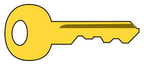
Pick a permutation π of $1, 2, \ldots, n$

The ciphertext is obtained by reading the columns from top to bottom, in the order given by π

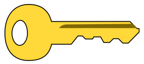
E.g., if the permutation is $4, 2, 1, 6, 5, 3$, then the ciphertext is:

$c =$ M G O T C H I O W D T T T O E E S R H X E I R T K E N M A O

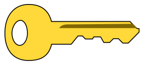
(Columnar) Transposition ciphers

What is the key? 

(Columnar) Transposition ciphers

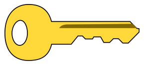
What is the key?  The pair (n, π)

(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

How do we decrypt the ciphertext?

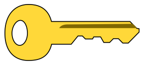
(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

How do we decrypt the ciphertext? Consider regular transposition ciphers, for convenience

- If the ciphertext has ℓ characters, then the original matrix had ℓ/n rows

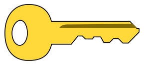
(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

How do we decrypt the ciphertext? Consider regular transposition ciphers, for convenience

- If the ciphertext has ℓ characters, then the original matrix had ℓ/n rows
- Write the ciphertext into columns of length ℓ/n, following the order given by π

(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

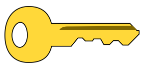
How do we decrypt the ciphertext? Consider regular transposition ciphers, for convenience

- If the ciphertext has ℓ characters, then the original matrix had ℓ/n rows
- Write the ciphertext into columns of length ℓ/n, following the order given by π

$c = \texttt{M G O T C H I O W D T T T O E E S R H X E I R T K E N M A O}$

$n = 6$, $\pi = (4, 2, 1, 6, 5, 3)$, $\ell = 30$

(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

How do we decrypt the ciphertext? Consider regular transposition ciphers, for convenience

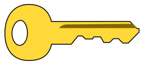
- If the ciphertext has ℓ characters, then the original matrix had ℓ/n rows
- Write the ciphertext into columns of length ℓ/n, following the order given by π

$c =$

M G O T C	H I O W D	T T T O E	E S R H X	E I R T K	E N M A O

$n = 6$, $\pi = (4, 2, 1, 6, 5, 3)$, $\ell = 30$

(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

How do we decrypt the ciphertext? Consider regular transposition ciphers, for convenience

- If the ciphertext has ℓ characters, then the original matrix had ℓ/n rows
- Write the ciphertext into columns of length ℓ/n, following the order given by π

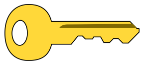
$c =$

M G O T C	H I O W D	T T T O E	E S R H X	E I R T K	E N M A O

$n = 6$, $\pi = (4, 2, 1, 6, 5, 3)$, $\ell = 30$

1	2	3	4	5	6
			M		
			G		
			O		
			T		
			C		

(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

How do we decrypt the ciphertext? Consider regular transposition ciphers, for convenience

- If the ciphertext has ℓ characters, then the original matrix had ℓ/n rows
- Write the ciphertext into columns of length ℓ/n, following the order given by π

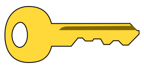
$c =$

M G O T C	H I O W D	T T T O E	E S R H X	E I R T K	E N M A O

$n = 6$, $\pi = (4, 2, 1, 6, 5, 3)$, $\ell = 30$

1	2	3	4	5	6
	H		M		
	I		G		
	O		O		
	W		T		
	D		C		

(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

How do we decrypt the ciphertext? Consider regular transposition ciphers, for convenience

- If the ciphertext has ℓ characters, then the original matrix had ℓ/n rows
- Write the ciphertext into columns of length ℓ/n, following the order given by π

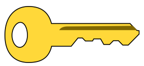
$c =$

M G O T C	H I O W D	T T T O E	E S R H X	E I R T K	E N M A O

$n = 6$, $\pi = (4, 2, 1, 6, 5, 3)$, $\ell = 30$

1	2	3	4	5	6
T	H		M		
T	I		G		
T	O		O		
O	W		T		
E	D		C		

(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

How do we decrypt the ciphertext? Consider regular transposition ciphers, for convenience

- If the ciphertext has ℓ characters, then the original matrix had ℓ/n rows
- Write the ciphertext into columns of length ℓ/n, following the order given by π

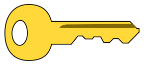
$c =$

M G O T C	H I O W D	T T T O E	E S R H X	E I R T K	E N M A O

$n = 6$, $\pi = (4, 2, 1, 6, 5, 3)$, $\ell = 30$

1	2	3	4	5	6
T	H		M		E
T	I		G		S
T	O		O		R
O	W		T		H
E	D		C		X

(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

How do we decrypt the ciphertext? Consider regular transposition ciphers, for convenience

- If the ciphertext has ℓ characters, then the original matrix had ℓ/n rows
- Write the ciphertext into columns of length ℓ/n, following the order given by π

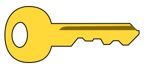
$c =$

M G O T C	H I O W D	T T T O E	E S R H X	E I R T K	E N M A O

$n = 6$, $\pi = (4, 2, 1, 6, 5, 3)$, $\ell = 30$

1	2	3	4	5	6
T	H		M	E	E
T	I		G	I	S
T	O		O	R	R
O	W		T	T	H
E	D		C	K	X

(Columnar) Transposition ciphers

What is the key?  The pair (n, π)

How do we decrypt the ciphertext? Consider regular transposition ciphers, for convenience

- If the ciphertext has ℓ characters, then the original matrix had ℓ/n rows
- Write the ciphertext into columns of length ℓ/n, following the order given by π

$c =$ `M G O T C | H I O W D | T T T O E | E S R H X | E I R T K | E N M A O`

$n = 6$, $\pi = (4, 2, 1, 6, 5, 3)$, $\ell = 30$

1	2	3	4	5	6
T	H	E	M	E	E
T	I	N	G	I	S
T	O	M	O	R	R
O	W	A	T	T	H
E	D	O	C	K	X

The plaintext can be found by reading the rows in order (left to right, top to bottom)

(Columnar) Transposition ciphers

Are columnar transposition ciphers secure?

(Columnar) Transposition ciphers

Are columnar transposition ciphers secure?

- Suppose that we already know the number n of columns (we can guess n)

  (if the transposition cipher is regular, look at the divisors of the ciphertext's length)

(Columnar) Transposition ciphers

Are columnar transposition ciphers secure?

- Suppose that we already know the number n of columns (we can guess n)
- How many keys do we still need to check?

(Columnar) Transposition ciphers

Are columnar transposition ciphers secure?

- Suppose that we already know the number n of columns (we can guess n)
- How many keys do we still need to check? $n!$

(Columnar) Transposition ciphers

Are columnar transposition ciphers secure?

- Suppose that we already know the number n of columns (we can guess n)
- How many keys do we still need to check? $n!$
- Brute force attacks are not feasible (for reasonable n)

(Columnar) Transposition ciphers

Are columnar transposition ciphers secure?

- Suppose that we already know the number n of columns (we can guess n)
- How many keys do we still need to check? $n!$
- Brute force attacks are not feasible (for reasonable n)

We can exploit the fact that transposition ciphers never change the plaintext characters (but only their order)

(Columnar) Transposition ciphers

Are columnar transposition ciphers secure?

- Suppose that we already know the number n of columns (we can guess n)
- How many keys do we still need to check? $n!$
- Brute force attacks are not feasible (for reasonable n)

We can exploit the fact that transposition ciphers never change the plaintext characters (but only their order)

- Write down the columns, in some arbitrary order (the permutation π is unknown)

```
E  E  E  H  T  M
N  I  S  I  T  G
M  R  R  O  T  O
A  T  H  W  O  T
O  K  X  D  E  C
```

(Columnar) Transposition ciphers

Are columnar transposition ciphers secure?

- Suppose that we already know the number n of columns (we can guess n)
- How many keys do we still need to check? $n!$
- Brute force attacks are not feasible (for reasonable n)

We can exploit the fact that transposition ciphers never change the plaintext characters (but only their order)

- Write down the columns, in some arbitrary order (the permutation π is unknown)

E	E	E	H	T	M
N	I	S	I	T	G
M	R	R	O	T	O
A	T	H	W	O	T
O	K	X	D	E	C

- Look for anagrams (that simultaneously yield intelligible text on multiple rows)

Other transposition ciphers

To make cryptanalysis harder, a double (irregular) transposition cipher is often used:

- Pick two sub-keys $k_1 = (n_1, \pi_1)$ and $k_2 = (n_2, \pi_2)$ $\qquad k = (k_1, k_2)$

Other transposition ciphers

To make cryptanalysis harder, a double (irregular) transposition cipher is often used:

- Pick two sub-keys $k_1 = (n_1, \pi_1)$ and $k_2 = (n_2, \pi_2)$ $\qquad k = (k_1, k_2)$
- Encrypt the plaintext m with k_1 a first time, to obtain c_1

Other transposition ciphers

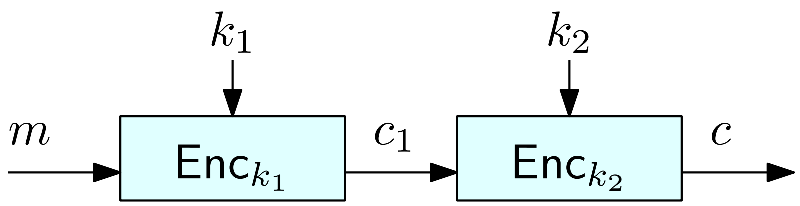
To make cryptanalysis harder, a double (irregular) transposition cipher is often used:

- Pick two sub-keys $k_1 = (n_1, \pi_1)$ and $k_2 = (n_2, \pi_2)$ $\qquad k = (k_1, k_2)$
- Encrypt the plaintext m with k_1 a first time, to obtain c_1
- Encrypt c_1 with k_2, to obtain the ciphertext c

Other transposition ciphers

To make cryptanalysis harder, a double (irregular) transposition cipher is often used:

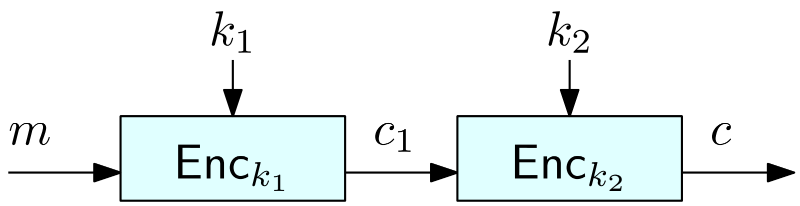
- Pick two sub-keys $k_1 = (n_1, \pi_1)$ and $k_2 = (n_2, \pi_2)$ $\qquad k = (k_1, k_2)$
- Encrypt the plaintext m with k_1 a first time, to obtain c_1
- Encrypt c_1 with k_2, to obtain the ciphertext c



Other transposition ciphers

To make cryptanalysis harder, a double (irregular) transposition cipher is often used:

- Pick two sub-keys $k_1 = (n_1, \pi_1)$ and $k_2 = (n_2, \pi_2)$ $\qquad k = (k_1, k_2)$
- Encrypt the plaintext m with k_1 a first time, to obtain c_1
- Encrypt c_1 with k_2, to obtain the ciphertext c

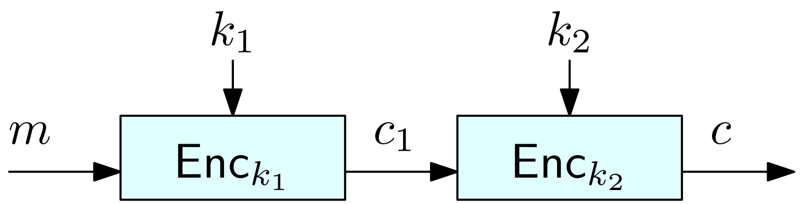


- Among the "manual" ciphers, the double transposition cipher is easy to carry out but hard to break

Other transposition ciphers

To make cryptanalysis harder, a double (irregular) transposition cipher is often used:

- Pick two sub-keys $k_1 = (n_1, \pi_1)$ and $k_2 = (n_2, \pi_2)$ $\qquad k = (k_1, k_2)$
- Encrypt the plaintext m with k_1 a first time, to obtain c_1
- Encrypt c_1 with k_2, to obtain the ciphertext c



- Among the "manual" ciphers, the double transposition cipher is easy to carry out but hard to break
- Many other (more complex) transposition ciphers have been used

Other transposition ciphers

The Zodiac Z-340 cipher remained unsolved for 51 years!

Other transposition ciphers

Ultimately, transposition ciphers are **not secure**:

- They never change the plaintext characters (but only permute their positions)

Other transposition ciphers

Ultimately, transposition ciphers are **not secure**:

- They never change the plaintext characters (but only permute their positions)
- Frequency analysis

Other transposition ciphers

Ultimately, transposition ciphers are **not secure**:

- They never change the plaintext characters (but only permute their positions)
- Frequency analysis
- If a key is close to the right one, a decryption of the ciphertext reveals parts of the plaintext

Other transposition ciphers

Ultimately, transposition ciphers are **not secure**:

- They never change the plaintext characters (but only permute their positions)
- Frequency analysis
- If a key is close to the right one, a decryption of the ciphertext reveals parts of the plaintext
- If a part of the plaintext is somehow known or guessed, this can be used to recover the key (known plaintext attack, key recovery attack)

Other transposition ciphers

Ultimately, transposition ciphers are **not secure**:

- They never change the plaintext characters (but only permute their positions)
- Frequency analysis
- If a key is close to the right one, a decryption of the ciphertext reveals parts of the plaintext
- If a part of the plaintext is somehow known or guessed, this can be used to recover the key (known plaintext attack, key recovery attack)

Are there even secure ciphers?

Other transposition ciphers

Ultimately, transposition ciphers are **not secure**:

- They never change the plaintext characters (but only permute their positions)
- Frequency analysis
- If a key is close to the right one, a decryption of the ciphertext reveals parts of the plaintext
- If a part of the plaintext is somehow known or guessed, this can be used to recover the key (known plaintext attack, key recovery attack)

Are there even secure ciphers?

What does secure mean?