When is an encryption scheme secure?

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$*,* **every** *message* $m \in \mathcal{M}$*, and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$*, and* **every** $c \in \mathcal{C}$*:*

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

Definition: *A private key encryption scheme* $\Pi = (Gen, Enc, Dec)$ *with message space* $\mathcal{M}$ *is* **perfectly indistinguishable** *if for every* $\mathcal{A}$ *it holds:*

$$\Pr[\mathit{PrivK}^{eav}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}$$

Is there a secure encryption scheme?

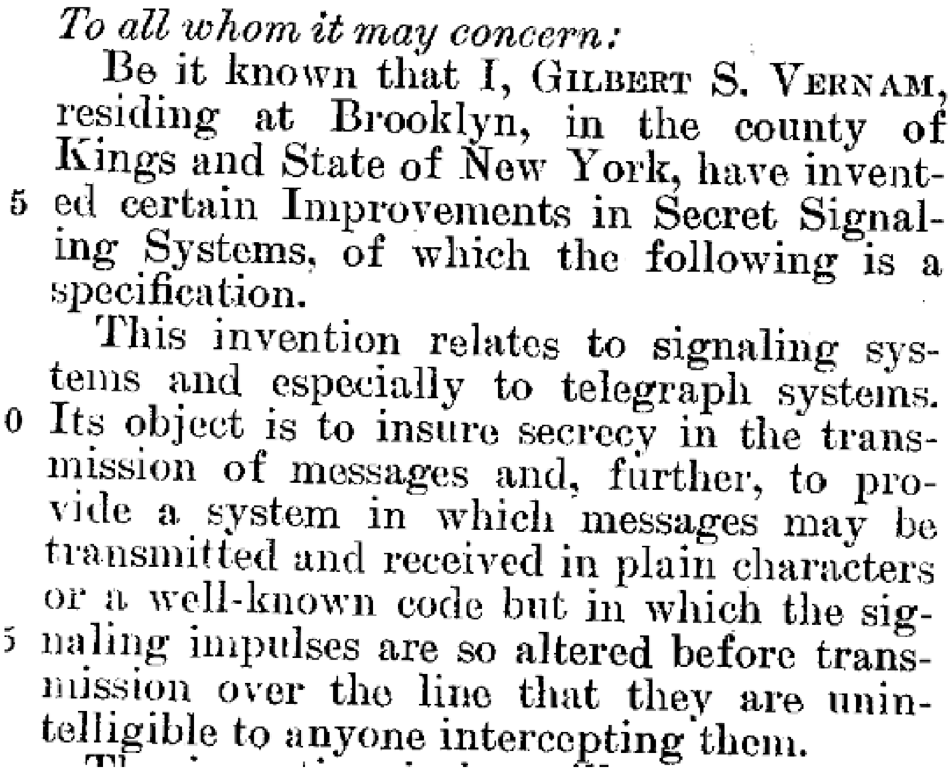
All the encryption schemes we have seen so fare are **not** secure according to our formal definitions

Is there a secure encryption scheme?

Is there a secure encryption scheme?

All the encryption schemes we have seen so fare are **not** secure according to our formal definitions

Is there a secure encryption scheme?



To all whom it may concern:

Be it known that I, GILBERT S. VERNAM, residing at Brooklyn, in the county of Kings and State of New York, have invented certain Improvements in Secret Signaling Systems, of which the following is a specification.

This invention relates to signaling systems and especially to telegraph systems. Its object is to insure secrecy in the transmission of messages and, further, to provide a system in which messages may be transmitted and received in plain characters or a well-known code but in which the signaling impulses are so altered before transmission over the line that they are unintelligible to anyone intercepting them.

Gilbert Vernam

Vernam Cipher

- Patented in 1917 by Gilbert Vernam with no proof of security

  (Shannon's definition of perfect secrecy is from 1949)
- Also called *one-time pad*
- Shannon subsequently proved that the cipher is perfectly secret
- $\oplus$ denotes the bitwise *exclusive or* (XOR) operator

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

Vernam Cipher

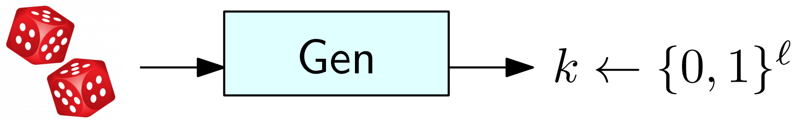
For an integer $\ell > 0$, the Vernam cipher is defined as follows:

- $\mathcal{M} = \{0,1\}^\ell, \quad \mathcal{C} = \{0,1\}^\ell, \quad \mathcal{K} = \{0,1\}^\ell$

Vernam Cipher

For an integer $\ell > 0$, the Vernam cipher is defined as follows:

- $\mathcal{M} = \{0,1\}^\ell, \quad \mathcal{C} = \{0,1\}^\ell, \quad \mathcal{K} = \{0,1\}^\ell$
- Gen: return a key k chosen uniformly at random from $\mathcal{K}$, i.e., $\Pr[K = k] = 2^{-\ell}\ \forall k$



Gen

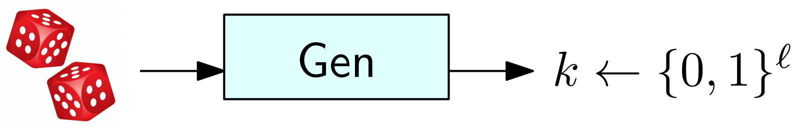
$k \leftarrow \{0,1\}^\ell$

Vernam Cipher

For an integer $\ell > 0$, the Vernam cipher is defined as follows:

- $\mathcal{M} = \{0,1\}^\ell$, $\mathcal{C} = \{0,1\}^\ell$, $\mathcal{K} = \{0,1\}^\ell$

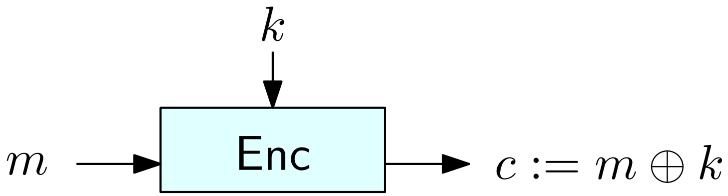
- Gen: return a key k chosen uniformly at random from $\mathcal{K}$, i.e., $\Pr[K = k] = 2^{-\ell}\ \forall k$



Gen

$k \leftarrow \{0,1\}^\ell$

- $\text{Enc}_k(m)$: return $c := k \oplus m$



k

m

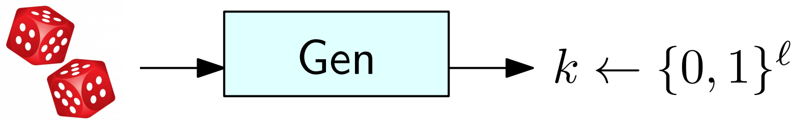
Enc

$c := m \oplus k$

Vernam Cipher

For an integer $\ell > 0$, the Vernam cipher is defined as follows:

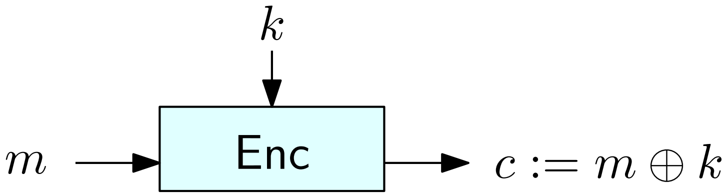
- $\mathcal{M} = \{0,1\}^\ell$, $\mathcal{C} = \{0,1\}^\ell$, $\mathcal{K} = \{0,1\}^\ell$
- Gen: return a key k chosen uniformly at random from $\mathcal{K}$, i.e., $\Pr[K = k] = 2^{-\ell}\ \forall k$



Gen

$k \leftarrow \{0,1\}^\ell$

- $\mathsf{Enc}_k(m)$: return $c := k \oplus m$



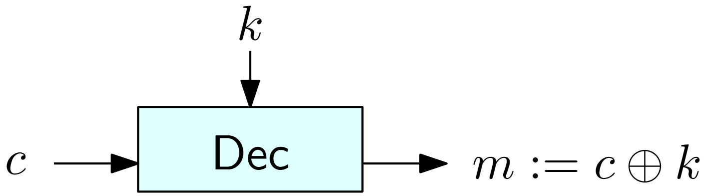
k

m

Enc

$c := m \oplus k$

- $\mathsf{Dec}_k(c)$: return $m := k \oplus c$



k

c

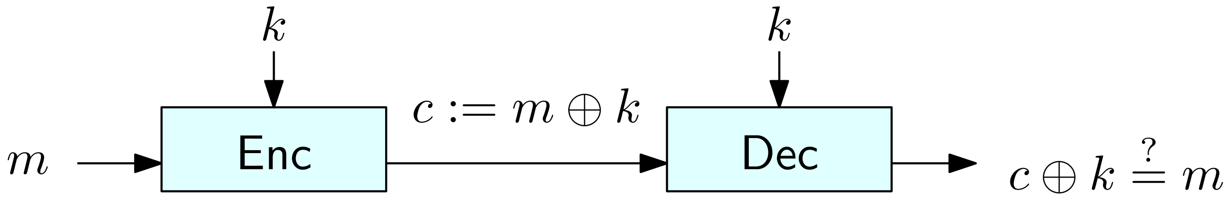
Dec

$m := c \oplus k$

Vernam Cipher

Is it correct?

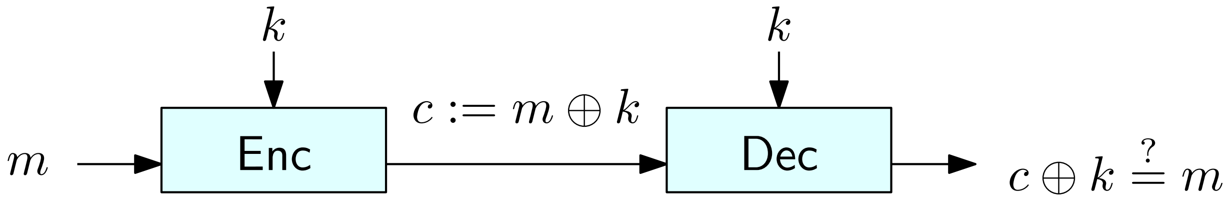
$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) \overset{?}{=} m$$



Vernam Cipher

Is it correct?

$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) \overset{?}{=} m$$


k

k

$c := m \oplus k$

m

Enc

Dec

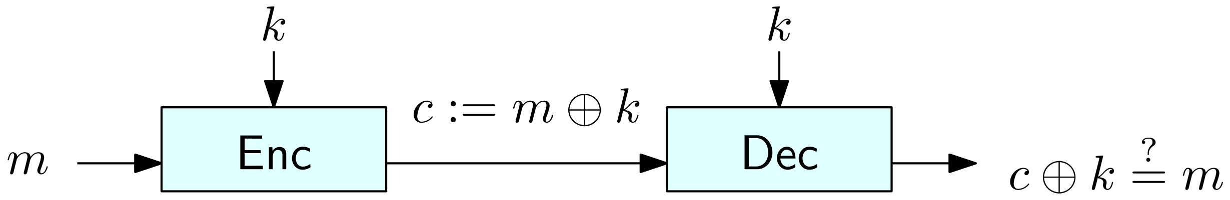
$c \oplus k \overset{?}{=} m$

$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) = \mathsf{Dec}_k(k \oplus m)$ (definition of Enc_k)

Vernam Cipher

Is it correct?

$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) \overset{?}{=} m$$



k k

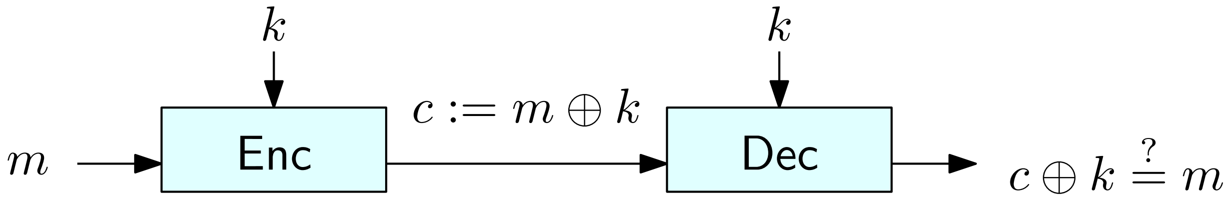
m Enc $c := m \oplus k$ Dec $c \oplus k \overset{?}{=} m$

$$\begin{aligned} \mathsf{Dec}_k(\mathsf{Enc}_k(m)) &= \mathsf{Dec}_k(k \oplus m) && \text{(definition of } \mathsf{Enc}_k\text{)} \\ &= k \oplus (k \oplus m) && \text{(definition of } \mathsf{Dec}_k\text{)} \end{aligned}$$

Vernam Cipher

Is it correct?

$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) \stackrel{?}{=} m$$

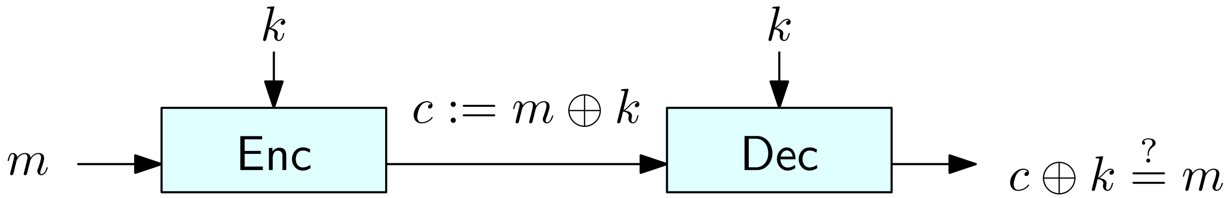


$$\begin{aligned}
\mathsf{Dec}_k(\mathsf{Enc}_k(m)) &= \mathsf{Dec}_k(k \oplus m) && \text{(definition of } \mathsf{Enc}_k\text{)}\\
&= k \oplus (k \oplus m) && \text{(definition of } \mathsf{Dec}_k\text{)}\\
&= (k \oplus k) \oplus m && \text{(associativity of } \oplus\text{)}
\end{aligned}$$

Vernam Cipher

Is it correct?

$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) \overset{?}{=} m$$



k

k

m

Enc

$c := m \oplus k$

Dec

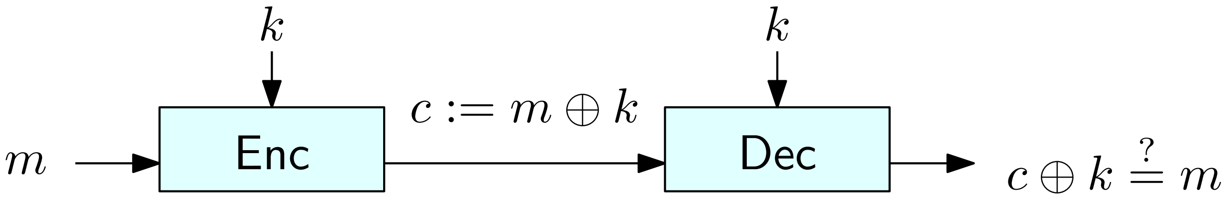
$c \oplus k \overset{?}{=} m$

$$\begin{aligned}
\mathsf{Dec}_k(\mathsf{Enc}_k(m)) &= \mathsf{Dec}_k(k \oplus m) && \text{(definition of } \mathsf{Enc}_k\text{)} \\
&= k \oplus (k \oplus m) && \text{(definition of } \mathsf{Dec}_k\text{)} \\
&= (k \oplus k) \oplus m && \text{(associativity of } \oplus\text{)} \\
&= \underbrace{00\ldots0}_{\ell \text{ times}} \oplus m && \text{(definition of } \oplus\text{)}
\end{aligned}$$

Vernam Cipher

Is it correct?

$$\mathsf{Dec}_k(\mathsf{Enc}_k(m)) \overset{?}{=} m$$



$$\begin{aligned}
\mathsf{Dec}_k(\mathsf{Enc}_k(m)) &= \mathsf{Dec}_k(k \oplus m) && \text{(definition of } \mathsf{Enc}_k\text{)} \\
&= k \oplus (k \oplus m) && \text{(definition of } \mathsf{Dec}_k\text{)} \\
&= (k \oplus k) \oplus m && \text{(associativity of } \oplus\text{)} \\
&= \underbrace{00\ldots0}_{\ell \text{ times}} \oplus m && \text{(definition of } \oplus\text{)} \\
&= m && \text{(definition of } \oplus\text{)}
\end{aligned}$$

Example

Alice wants to send a message $m = \texttt{001010}$ of $\ell = 6$ bits to Bob. Alice and Bob agreed to use a Vernam cipher and have already exchanged a key $k = \texttt{101101}$

What is the ciphertext c?

$$
\begin{array}{r}
m = \texttt{0 0 1 0 1 0} \quad \oplus \\
k = \texttt{1 0 1 1 0 1} \quad = \\
\hline
c = \texttt{1 0 0 1 1 1}
\end{array}
$$

Example

Alice wants to send a message $m = 001010$ of $\ell = 6$ bits to Bob. Alice and Bob agreed to use a Vernam cipher and have already exchanged a key $k = 101101$

What is the ciphertext c?

$$\begin{array}{rcccccccl} m = & 0 & 0 & 1 & 0 & 1 & 0 & & \oplus \\ k = & 1 & 0 & 1 & 1 & 0 & 1 & & = \\ \hline c = & 1 & 0 & 0 & 1 & 1 & 1 & & \end{array}$$

Bob receives the ciphetext $c = 110101$ from Alice. Alice and Bob have agreed to use a Vernam cipher with key $k = 000110$

What is the plaintext m?

$$\begin{array}{rcccccccl} c = & 1 & 1 & 0 & 1 & 0 & 1 & & \oplus \\ k = & 0 & 0 & 0 & 1 & 1 & 0 & & = \\ \hline m = & 1 & 1 & 0 & 0 & 1 & 0 & & \end{array}$$

Encoding

- The historic ciphers were defined over the Latin alphabet $\{\mathtt{a}, \ldots, \mathtt{z}\}$
- The Vernam cipher is defined over the binary alphabet $\{\mathtt{0,\ 1}\}$

Encoding

- The historic ciphers were defined over the Latin alphabet $\{\mathtt{a}, \ldots, \mathtt{z}\}$
- The Vernam cipher is defined over the binary alphabet $\{\mathtt{0,\ 1}\}$

How do we send messages using the Latin (or any other) alphabet?

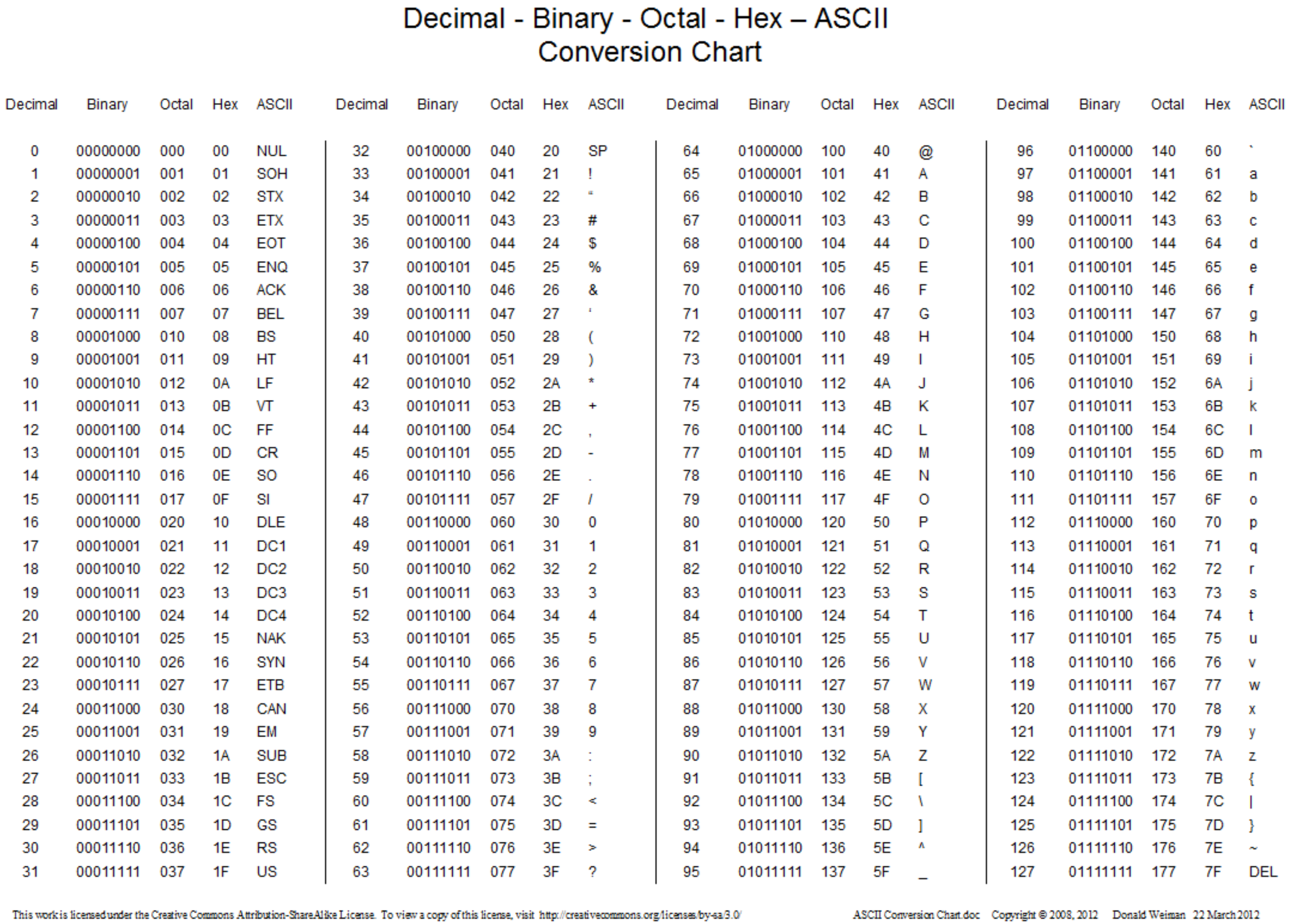
Encoding

- The historic ciphers were defined over the Latin alphabet $\{\texttt{a}, \dots, \texttt{z}\}$
- The Vernam cipher is defined over the binary alphabet $\{\texttt{0, 1}\}$

How do we send messages using the Latin (or any other) alphabet?

- We can always encode the symbols in the message alphabet in binary on Alice's side (before encryption)...
- ...and decode them on Bob's side (after decryption)

Encoding



Decimal - Binary - Octal - Hex – ASCII Conversion Chart

Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII
0	00000000	000	00	NUL	32	00100000	040	20	SP	64	01000000	100	40	@	96	01100000	140	60	`
1	00000001	001	01	SOH	33	00100001	041	21	!	65	01000001	101	41	A	97	01100001	141	61	a
2	00000010	002	02	STX	34	00100010	042	22	"	66	01000010	102	42	B	98	01100010	142	62	b
3	00000011	003	03	ETX	35	00100011	043	23	#	67	01000011	103	43	C	99	01100011	143	63	c
4	00000100	004	04	EOT	36	00100100	044	24	$	68	01000100	104	44	D	100	01100100	144	64	d
5	00000101	005	05	ENQ	37	00100101	045	25	%	69	01000101	105	45	E	101	01100101	145	65	e
6	00000110	006	06	ACK	38	00100110	046	26	&	70	01000110	106	46	F	102	01100110	146	66	f
7	00000111	007	07	BEL	39	00100111	047	27	'	71	01000111	107	47	G	103	01100111	147	67	g
8	00001000	010	08	BS	40	00101000	050	28	(	72	01001000	110	48	H	104	01101000	150	68	h
9	00001001	011	09	HT	41	00101001	051	29	)	73	01001001	111	49	I	105	01101001	151	69	i
10	00001010	012	0A	LF	42	00101010	052	2A	*	74	01001010	112	4A	J	106	01101010	152	6A	j
11	00001011	013	0B	VT	43	00101011	053	2B	+	75	01001011	113	4B	K	107	01101011	153	6B	k
12	00001100	014	0C	FF	44	00101100	054	2C	,	76	01001100	114	4C	L	108	01101100	154	6C	l
13	00001101	015	0D	CR	45	00101101	055	2D	-	77	01001101	115	4D	M	109	01101101	155	6D	m
14	00001110	016	0E	SO	46	00101110	056	2E	.	78	01001110	116	4E	N	110	01101110	156	6E	n
15	00001111	017	0F	SI	47	00101111	057	2F	/	79	01001111	117	4F	O	111	01101111	157	6F	o
16	00010000	020	10	DLE	48	00110000	060	30	0	80	01010000	120	50	P	112	01110000	160	70	p
17	00010001	021	11	DC1	49	00110001	061	31	1	81	01010001	121	51	Q	113	01110001	161	71	q
18	00010010	022	12	DC2	50	00110010	062	32	2	82	01010010	122	52	R	114	01110010	162	72	r
19	00010011	023	13	DC3	51	00110011	063	33	3	83	01010011	123	53	S	115	01110011	163	73	s
20	00010100	024	14	DC4	52	00110100	064	34	4	84	01010100	124	54	T	116	01110100	164	74	t
21	00010101	025	15	NAK	53	00110101	065	35	5	85	01010101	125	55	U	117	01110101	165	75	u
22	00010110	026	16	SYN	54	00110110	066	36	6	86	01010110	126	56	V	118	01110110	166	76	v
23	00010111	027	17	ETB	55	00110111	067	37	7	87	01010111	127	57	W	119	01110111	167	77	w
24	00011000	030	18	CAN	56	00111000	070	38	8	88	01011000	130	58	X	120	01111000	170	78	x
25	00011001	031	19	EM	57	00111001	071	39	9	89	01011001	131	59	Y	121	01111001	171	79	y
26	00011010	032	1A	SUB	58	00111010	072	3A	:	90	01011010	132	5A	Z	122	01111010	172	7A	z
27	00011011	033	1B	ESC	59	00111011	073	3B	;	91	01011011	133	5B	[	123	01111011	173	7B	{
28	00011100	034	1C	FS	60	00111100	074	3C	<	92	01011100	134	5C	\	124	01111100	174	7C	|
29	00011101	035	1D	GS	61	00111101	075	3D	=	93	01011101	135	5D	]	125	01111101	175	7D	}
30	00011110	036	1E	RS	62	00111110	076	3E	>	94	01011110	136	5E	^	126	01111110	176	7E	~
31	00011111	037	1F	US	63	00111111	077	3F	?	95	01011111	137	5F	_	127	01111111	177	7F	DEL

Proof of security

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$*,* **every** *message* $m \in \mathcal{M}$*, and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$*, and* **every** $c \in \mathcal{C}$*:*

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

Definition: *A private key encryption scheme* $\Pi = (Gen, Enc, Dec)$ *with message space* $\mathcal{M}$ *is* **perfectly indistinguishable** *if for every* $\mathcal{A}$ *it holds:*

$$\Pr[\mathit{PrivK}^{eav}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}$$

Proof of security

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** *probability distribution over* $\mathcal{M}$, **every** *message* $m \in \mathcal{M}$, *and* **every** *ciphertext* $c \in \mathcal{C}$ *with* $\Pr[C = c] \neq 0$*:*

$$\Pr[M = m \mid C = c] = \Pr[M = m]$$

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$*:*

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

Definition: *A private key encryption scheme* $\Pi = (Gen, Enc, Dec)$ *with message space* $\mathcal{M}$ *is* **perfectly indistinguishable** *if for every* $\mathcal{A}$ *it holds:*

$$\Pr[\mathit{PrivK}^{eav}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}$$

Proof of security

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$*:*

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof of security

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$*:*

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof:

For any $m, m' \in \mathcal{M}, c \in \mathcal{C}$:

Proof of security

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$:

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof:

For any $m, m' \in \mathcal{M}, c \in \mathcal{C}$:

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[K \oplus m = c]$$

Proof of security

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$*:*

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof:

For any $m, m' \in \mathcal{M}, c \in \mathcal{C}$:

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[K \oplus m = c]$$

$$= \Pr[K = c \oplus m]$$

Proof of security

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$:

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof:

For any $m, m' \in \mathcal{M}, c \in \mathcal{C}$:

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[K \oplus m = c]$$

$$= \Pr[K = c \oplus m] \ = 2^{-\ell}$$

Proof of security

Definition: *An encryption scheme* (Gen, Enc, Dec) *with message space* $\mathcal{M}$ *is* **perfectly secret** *if* **for every** $m, m' \in \mathcal{M}$, *and* **every** $c \in \mathcal{C}$*:*

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$$

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof:

For any $m, m' \in \mathcal{M}, c \in \mathcal{C}$:

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[K \oplus m = c]$$

$$= \Pr[K = c \oplus m] = 2^{-\ell} = \Pr[K = c \oplus m']$$

$$= \Pr[K \oplus m' = c] = \Pr[\mathsf{Enc}_K(m') = c]$$

$\square$

Caveats & Limitations of One-time Pad

- The key must be (at least) as long as the message

Caveats & Limitations of One-time Pad

- The key must be (at least) as long as the message
- Pre-sharing a long key is difficult

Caveats & Limitations of One-time Pad

- The key must be (at least) as long as the message
- Pre-sharing a long key is difficult
- The key must be stored securely

(e.g., how would you handle full-disk encryption?)

Caveats & Limitations of One-time Pad

- The key must be (at least) as long as the message
- Pre-sharing a long key is difficult
- The key must be stored securely

  (e.g., how would you handle full-disk encryption?)
- The bits of the key must be generated independently and uniformly at random

Caveats & Limitations of One-time Pad

- The key must be (at least) as long as the message
- Pre-sharing a long key is difficult
- The key must be stored securely

  (e.g., how would you handle full-disk encryption?)
- The bits of the key must be generated independently and uniformly at random
- **The key must never be reused (not even partially!)**

> *You should never re-use a one-time pad. It's like toilet paper; if you re-use it, things get messy.*
>
> – Michael Rabin

Caveats & Limitations of One-time Pad

What happens if a key is reused?

- $c_1 = \mathsf{Enc}_k(m_1)$
- $c_2 = \mathsf{Enc}_k(m_2)$

Caveats & Limitations of One-time Pad

What happens if a key is reused?

- $c_1 = \mathsf{Enc}_k(m_1)$
- $c_2 = \mathsf{Enc}_k(m_2)$

The adversary can compute $c_1 \oplus c_2$

Caveats & Limitations of One-time Pad

What happens if a key is reused?

- $c_1 = \mathsf{Enc}_k(m_1)$
- $c_2 = \mathsf{Enc}_k(m_2)$

The adversary can compute $c_1 \oplus c_2$

$c_1 \oplus c_2 = (k \oplus m_1) \oplus (k \oplus m_2)$

Caveats & Limitations of One-time Pad

What happens if a key is reused?

- $c_1 = \mathsf{Enc}_k(m_1)$
- $c_2 = \mathsf{Enc}_k(m_2)$

The adversary can compute $c_1 \oplus c_2$

$$\begin{aligned} c_1 \oplus c_2 &= (k \oplus m_1) \oplus (k \oplus m_2) \\ &= m_1 \oplus (k \oplus k) \oplus m_2 && \text{(commutativity + associativity)} \end{aligned}$$

Caveats & Limitations of One-time Pad

What happens if a key is reused?

- $c_1 = \mathsf{Enc}_k(m_1)$
- $c_2 = \mathsf{Enc}_k(m_2)$

The adversary can compute $c_1 \oplus c_2$

$$
\begin{aligned}
c_1 \oplus c_2 &= (k \oplus m_1) \oplus (k \oplus m_2) \\
&= m_1 \oplus (k \oplus k) \oplus m_2 && \text{(commutativity + associativity)} \\
&= m_1 \oplus 0 \ldots 0 \oplus m_2 && \text{(definition of } \oplus\text{)}
\end{aligned}
$$

Caveats & Limitations of One-time Pad

What happens if a key is reused?

- $c_1 = \mathsf{Enc}_k(m_1)$
- $c_2 = \mathsf{Enc}_k(m_2)$

The adversary can compute $c_1 \oplus c_2$

$$
\begin{aligned}
c_1 \oplus c_2 &= (k \oplus m_1) \oplus (k \oplus m_2) \\
&= m_1 \oplus (k \oplus k) \oplus m_2 && \text{(commutativity + associativity)} \\
&= m_1 \oplus 0 \ldots 0 \oplus m_2 && \text{(definition of } \oplus\text{)} \\
&= m_1 \oplus m_2 && \text{(definition of } \oplus\text{)}
\end{aligned}
$$

The adversary learns $m_1 \oplus m_2$

Caveats & Limitations of One-time Pad

What happens if a key is reused?

- $c_1 = \mathsf{Enc}_k(m_1)$
- $c_2 = \mathsf{Enc}_k(m_2)$

The adversary can compute $c_1 \oplus c_2$

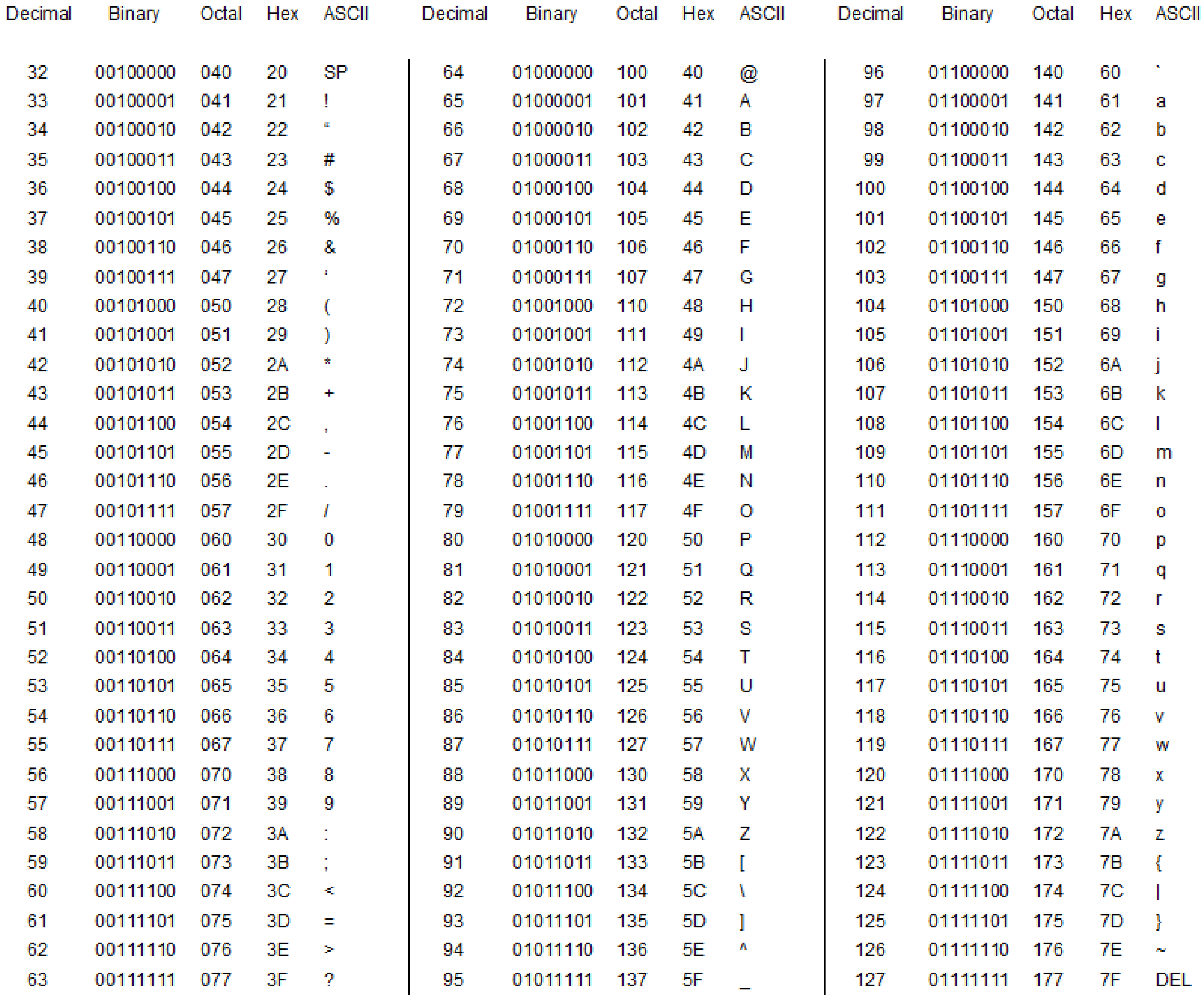
$$\begin{aligned} c_1 \oplus c_2 &= (k \oplus m_1) \oplus (k \oplus m_2) \\ &= m_1 \oplus (k \oplus k) \oplus m_2 && \text{(commutativity + associativity)} \\ &= m_1 \oplus 0 \ldots 0 \oplus m_2 && \text{(definition of } \oplus\text{)} \\ &= m_1 \oplus m_2 && \text{(definition of } \oplus\text{)} \end{aligned}$$

The adversary learns $m_1 \oplus m_2$

Do we care?

Caveats & Limitations of One-time Pad

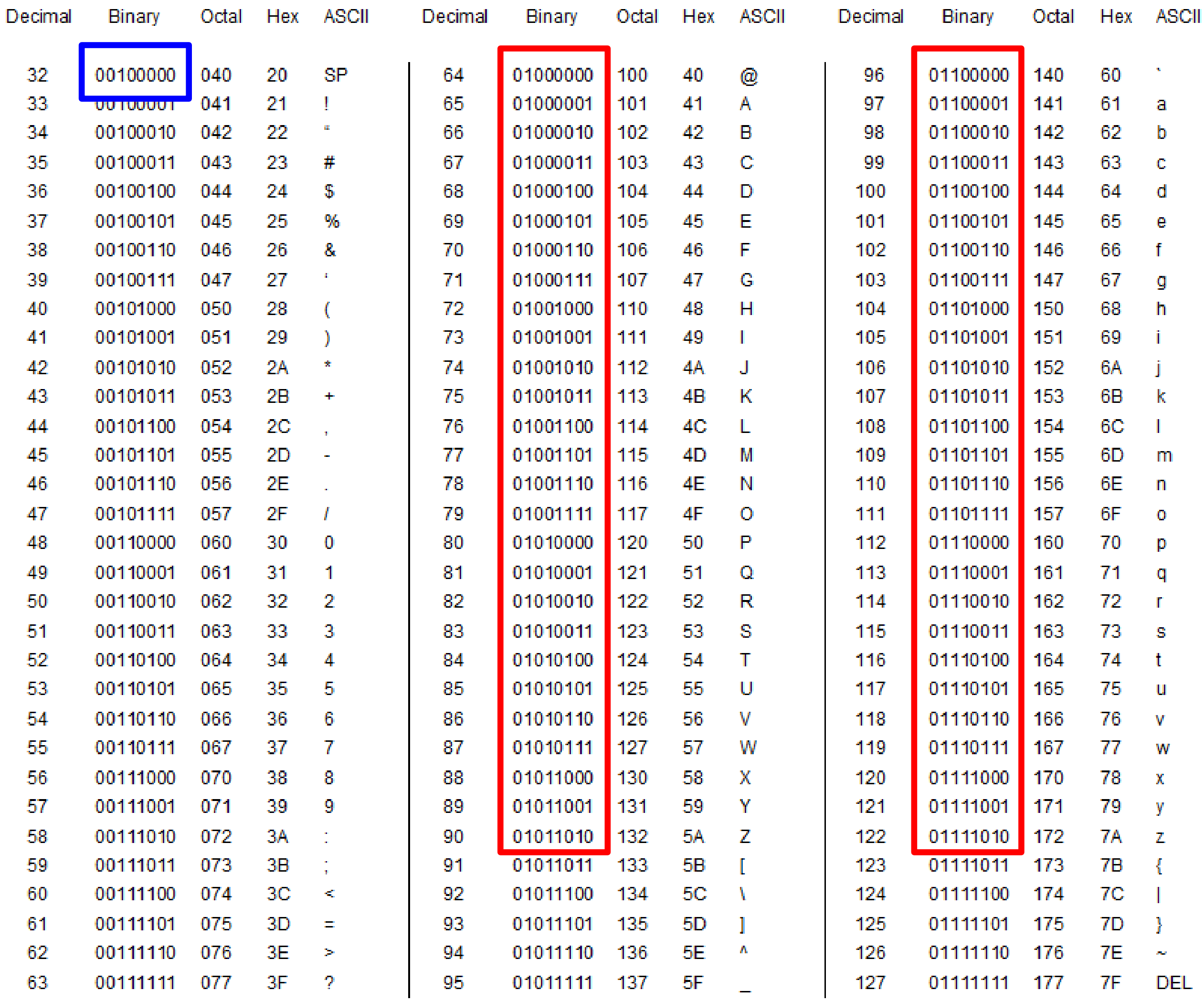
- Frequency analysis!
  (e.g., e $\oplus$ e $= 0 \ldots 0$)



Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII
32	00100000	040	20	SP	64	01000000	100	40	@	96	01100000	140	60	`
33	00100001	041	21	!	65	01000001	101	41	A	97	01100001	141	61	a
34	00100010	042	22	"	66	01000010	102	42	B	98	01100010	142	62	b
35	00100011	043	23	#	67	01000011	103	43	C	99	01100011	143	63	c
36	00100100	044	24	$	68	01000100	104	44	D	100	01100100	144	64	d
37	00100101	045	25	%	69	01000101	105	45	E	101	01100101	145	65	e
38	00100110	046	26	&	70	01000110	106	46	F	102	01100110	146	66	f
39	00100111	047	27	'	71	01000111	107	47	G	103	01100111	147	67	g
40	00101000	050	28	(	72	01001000	110	48	H	104	01101000	150	68	h
41	00101001	051	29	)	73	01001001	111	49	I	105	01101001	151	69	i
42	00101010	052	2A	*	74	01001010	112	4A	J	106	01101010	152	6A	j
43	00101011	053	2B	+	75	01001011	113	4B	K	107	01101011	153	6B	k
44	00101100	054	2C	,	76	01001100	114	4C	L	108	01101100	154	6C	l
45	00101101	055	2D	-	77	01001101	115	4D	M	109	01101101	155	6D	m
46	00101110	056	2E	.	78	01001110	116	4E	N	110	01101110	156	6E	n
47	00101111	057	2F	/	79	01001111	117	4F	O	111	01101111	157	6F	o
48	00110000	060	30	0	80	01010000	120	50	P	112	01110000	160	70	p
49	00110001	061	31	1	81	01010001	121	51	Q	113	01110001	161	71	q
50	00110010	062	32	2	82	01010010	122	52	R	114	01110010	162	72	r
51	00110011	063	33	3	83	01010011	123	53	S	115	01110011	163	73	s
52	00110100	064	34	4	84	01010100	124	54	T	116	01110100	164	74	t
53	00110101	065	35	5	85	01010101	125	55	U	117	01110101	165	75	u
54	00110110	066	36	6	86	01010110	126	56	V	118	01110110	166	76	v
55	00110111	067	37	7	87	01010111	127	57	W	119	01110111	167	77	w
56	00111000	070	38	8	88	01011000	130	58	X	120	01111000	170	78	x
57	00111001	071	39	9	89	01011001	131	59	Y	121	01111001	171	79	y
58	00111010	072	3A	:	90	01011010	132	5A	Z	122	01111010	172	7A	z
59	00111011	073	3B	;	91	01011011	133	5B	[	123	01111011	173	7B	{
60	00111100	074	3C	<	92	01011100	134	5C	\	124	01111100	174	7C	|
61	00111101	075	3D	=	93	01011101	135	5D	]	125	01111101	175	7D	}
62	00111110	076	3E	>	94	01011110	136	5E	^	126	01111110	176	7E	~
63	00111111	077	3F	?	95	01011111	137	5F	_	127	01111111	177	7F	DEL

Caveats & Limitations of One-time Pad

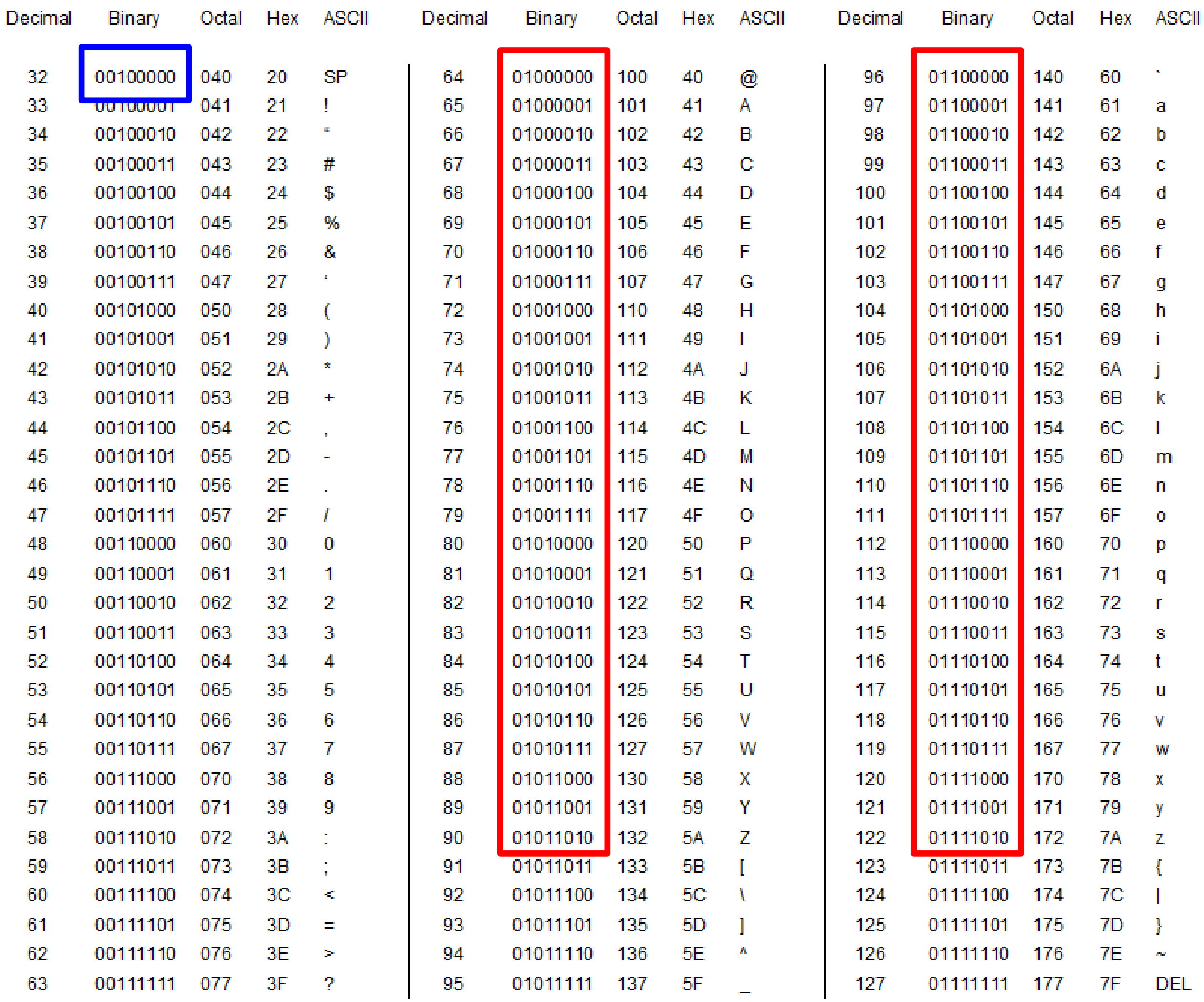
- Frequency analysis!
  (e.g., $\mathrm{e} \oplus \mathrm{e} = 0 \ldots 0$)
- Patterns in the ASCII encoding
  - The encoding of all letters starts with $01\ldots$
  - The encoding of a space starts with $00\ldots$



Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII
32	00100000	040	20	SP	64	01000000	100	40	@	96	01100000	140	60	`
33	00100001	041	21	!	65	01000001	101	41	A	97	01100001	141	61	a
34	00100010	042	22	"	66	01000010	102	42	B	98	01100010	142	62	b
35	00100011	043	23	#	67	01000011	103	43	C	99	01100011	143	63	c
36	00100100	044	24	$	68	01000100	104	44	D	100	01100100	144	64	d
37	00100101	045	25	%	69	01000101	105	45	E	101	01100101	145	65	e
38	00100110	046	26	&	70	01000110	106	46	F	102	01100110	146	66	f
39	00100111	047	27	'	71	01000111	107	47	G	103	01100111	147	67	g
40	00101000	050	28	(	72	01001000	110	48	H	104	01101000	150	68	h
41	00101001	051	29	)	73	01001001	111	49	I	105	01101001	151	69	i
42	00101010	052	2A	*	74	01001010	112	4A	J	106	01101010	152	6A	j
43	00101011	053	2B	+	75	01001011	113	4B	K	107	01101011	153	6B	k
44	00101100	054	2C	,	76	01001100	114	4C	L	108	01101100	154	6C	l
45	00101101	055	2D	-	77	01001101	115	4D	M	109	01101101	155	6D	m
46	00101110	056	2E	.	78	01001110	116	4E	N	110	01101110	156	6E	n
47	00101111	057	2F	/	79	01001111	117	4F	O	111	01101111	157	6F	o
48	00110000	060	30	0	80	01010000	120	50	P	112	01110000	160	70	p
49	00110001	061	31	1	81	01010001	121	51	Q	113	01110001	161	71	q
50	00110010	062	32	2	82	01010010	122	52	R	114	01110010	162	72	r
51	00110011	063	33	3	83	01010011	123	53	S	115	01110011	163	73	s
52	00110100	064	34	4	84	01010100	124	54	T	116	01110100	164	74	t
53	00110101	065	35	5	85	01010101	125	55	U	117	01110101	165	75	u
54	00110110	066	36	6	86	01010110	126	56	V	118	01110110	166	76	v
55	00110111	067	37	7	87	01010111	127	57	W	119	01110111	167	77	w
56	00111000	070	38	8	88	01011000	130	58	X	120	01111000	170	78	x
57	00111001	071	39	9	89	01011001	131	59	Y	121	01111001	171	79	y
58	00111010	072	3A	:	90	01011010	132	5A	Z	122	01111010	172	7A	z
59	00111011	073	3B	;	91	01011011	133	5B	[	123	01111011	173	7B	{
60	00111100	074	3C	<	92	01011100	134	5C	\	124	01111100	174	7C	|
61	00111101	075	3D	=	93	01011101	135	5D	]	125	01111101	175	7D	}
62	00111110	076	3E	>	94	01011110	136	5E	^	126	01111110	176	7E	~
63	00111111	077	3F	?	95	01011111	137	5F	_	127	01111111	177	7F	DEL

Caveats & Limitations of One-time Pad

- Frequency analysis!
  (e.g., $\text{e} \oplus \text{e} = 0 \ldots 0$)
- Patterns in the ASCII encoding
  - The encoding of all letters starts with $01\ldots$
  - The encoding of a space starts with $00\ldots$
  - Trivial to identify the exclusive-or of letter and space!



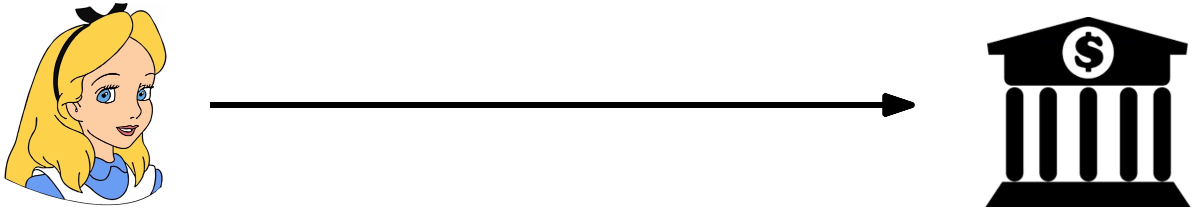
Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII
32	00100000	040	20	SP	64	01000000	100	40	@	96	01100000	140	60	`
33	00100001	041	21	!	65	01000001	101	41	A	97	01100001	141	61	a
34	00100010	042	22	"	66	01000010	102	42	B	98	01100010	142	62	b
35	00100011	043	23	#	67	01000011	103	43	C	99	01100011	143	63	c
36	00100100	044	24	$	68	01000100	104	44	D	100	01100100	144	64	d
37	00100101	045	25	%	69	01000101	105	45	E	101	01100101	145	65	e
38	00100110	046	26	&	70	01000110	106	46	F	102	01100110	146	66	f
39	00100111	047	27	'	71	01000111	107	47	G	103	01100111	147	67	g
40	00101000	050	28	(	72	01001000	110	48	H	104	01101000	150	68	h
41	00101001	051	29	)	73	01001001	111	49	I	105	01101001	151	69	i
42	00101010	052	2A	*	74	01001010	112	4A	J	106	01101010	152	6A	j
43	00101011	053	2B	+	75	01001011	113	4B	K	107	01101011	153	6B	k
44	00101100	054	2C	,	76	01001100	114	4C	L	108	01101100	154	6C	l
45	00101101	055	2D	-	77	01001101	115	4D	M	109	01101101	155	6D	m
46	00101110	056	2E	.	78	01001110	116	4E	N	110	01101110	156	6E	n
47	00101111	057	2F	/	79	01001111	117	4F	O	111	01101111	157	6F	o
48	00110000	060	30	0	80	01010000	120	50	P	112	01110000	160	70	p
49	00110001	061	31	1	81	01010001	121	51	Q	113	01110001	161	71	q
50	00110010	062	32	2	82	01010010	122	52	R	114	01110010	162	72	r
51	00110011	063	33	3	83	01010011	123	53	S	115	01110011	163	73	s
52	00110100	064	34	4	84	01010100	124	54	T	116	01110100	164	74	t
53	00110101	065	35	5	85	01010101	125	55	U	117	01110101	165	75	u
54	00110110	066	36	6	86	01010110	126	56	V	118	01110110	166	76	v
55	00110111	067	37	7	87	01010111	127	57	W	119	01110111	167	77	w
56	00111000	070	38	8	88	01011000	130	58	X	120	01111000	170	78	x
57	00111001	071	39	9	89	01011001	131	59	Y	121	01111001	171	79	y
58	00111010	072	3A	:	90	01011010	132	5A	Z	122	01111010	172	7A	z
59	00111011	073	3B	;	91	01011011	133	5B	[	123	01111011	173	7B	{
60	00111100	074	3C	<	92	01011100	134	5C	\	124	01111100	174	7C	|
61	00111101	075	3D	=	93	01011101	135	5D	]	125	01111101	175	7D	}
62	00111110	076	3E	>	94	01011110	136	5E	^	126	01111110	176	7E	~
63	00111111	077	3F	?	95	01011111	137	5F	_	127	01111111	177	7F	DEL

Caveats & Limitations of One-time Pad

- Alice buys an item from the adversary for 5.20€

Caveats & Limitations of One-time Pad

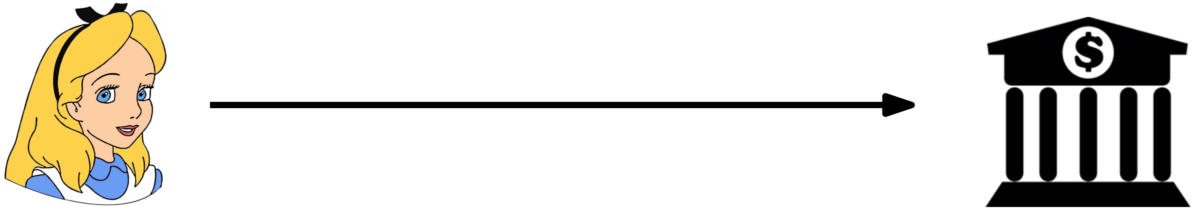
- Alice buys an item from the adversary for 5.20€
- Alice makes a wire transfer from her bank's website



Caveats & Limitations of One-time Pad

- Alice buys an item from the adversary for 5.20€
- Alice makes a wire transfer from her bank's website
- The bank website sends a message of the form `PAY <RECIPIENT_IBAN> <AMOUNT>` to the bank's backend

$$m = \underbrace{010100000100000101011001}_{\texttt{PAY}}\,\underbrace{01001001\ldots00110010}_{\texttt{IBAN}}\,\underbrace{0000000100000100}_{\texttt{AMOUNT (520)}}$$

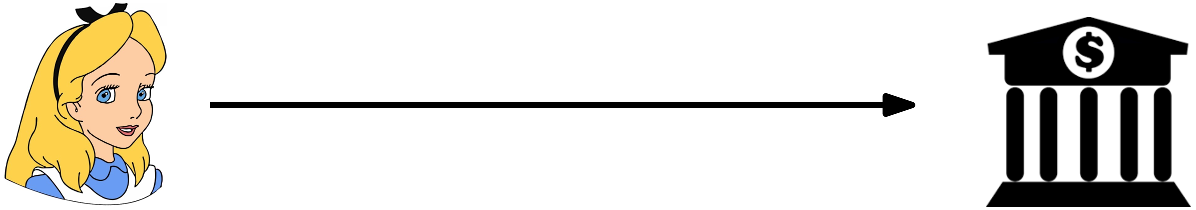


Caveats & Limitations of One-time Pad

- Alice buys an item from the adversary for 5.20€
- Alice makes a wire transfer from her bank's website
- The bank website sends a message of the form `PAY <RECIPIENT_IBAN> <AMOUNT>` to the bank's backend

$$m = \underbrace{\texttt{010100000100000101011001}}_{\texttt{PAY}}\,\underbrace{\texttt{01001001}\ldots\texttt{00110010}}_{\texttt{IBAN}}\,\underbrace{\texttt{0000000100000100}}_{\texttt{AMOUNT (520)}}$$

- The message is encrypted with a one-time pad



Caveats & Limitations of One-time Pad

- Alice buys an item from the adversary for 5.20€
- Alice makes a wire transfer from her bank's website
- The bank website sends a message of the form `PAY <RECIPIENT_IBAN> <AMOUNT>` to the bank's backend

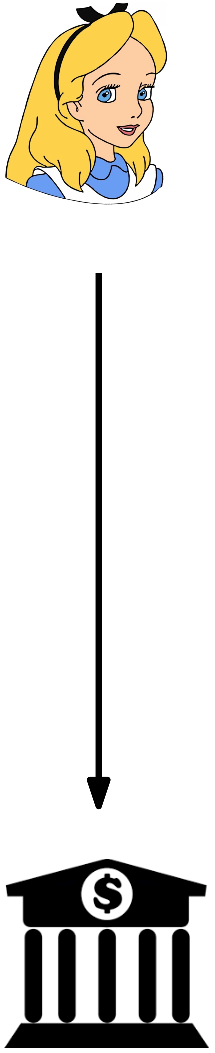
$$m = \underbrace{010100000100000101011001}_{\texttt{PAY}}\underbrace{01001001\ldots00110010}_{\texttt{IBAN}}\underbrace{0000000100000100}_{\texttt{AMOUNT (520)}}$$

- The message is encrypted with a one-time pad

Caveats & Limitations of One-time Pad

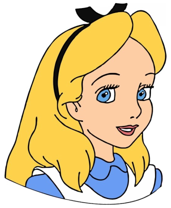
$$m = \underbrace{\texttt{010100000100000101011001}}_{\texttt{PAY}}\underbrace{\texttt{01001001}\ldots\texttt{00110010}}_{\texttt{IBAN}}\underbrace{\texttt{0000000100000100}}_{\texttt{AMOUNT (520)}}$$

$$c = \underbrace{\texttt{0011011000101010000110101}}_{\texttt{PAY}}\underbrace{\texttt{11010001}\ldots\texttt{10001101}}_{\texttt{IBAN}}\underbrace{\texttt{1011111010010010}}_{\texttt{AMOUNT}}$$



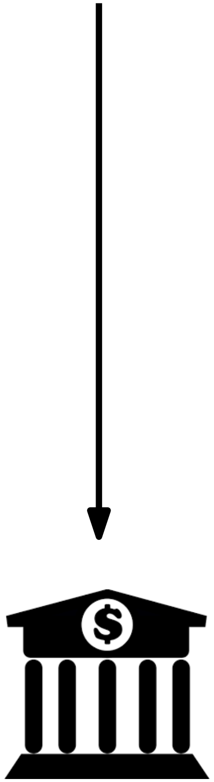
Caveats & Limitations of One-time Pad

$$m = \underbrace{010100000100000101011001}_{\texttt{PAY}}\underbrace{01001001\ldots00110010}_{\texttt{IBAN}}\underbrace{0000000100000100}_{\texttt{AMOUNT (520)}}$$

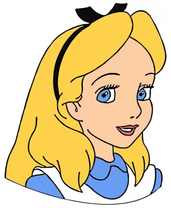


$$c = \underbrace{0011011000101010000110101}_{\texttt{PAY}}\underbrace{11010001\ldots10001101}_{\texttt{IBAN}}\underbrace{1011111010010010}_{\texttt{AMOUNT}}$$

$$\oplus \qquad \ldots 1000000000000000$$



Caveats & Limitations of One-time Pad



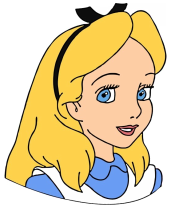
$$m = \underbrace{\texttt{010100000100000101011001}}_{\texttt{PAY}}\underbrace{\texttt{01001001}\ldots\texttt{00110010}}_{\texttt{IBAN}}\underbrace{\texttt{0000000100000100}}_{\texttt{AMOUNT (520)}}$$

$$c = \underbrace{\texttt{0011011000101010000110101}}_{\texttt{PAY}}\underbrace{\texttt{11010001}\ldots\texttt{10001101}}_{\texttt{IBAN}}\underbrace{\texttt{1011111010010010}}_{\texttt{AMOUNT}}$$

$$\oplus \qquad \ldots\texttt{1000000000000000}$$

$$c' = \underbrace{\texttt{0011011000101010000110101}}_{\texttt{PAY}}\underbrace{\texttt{11010001}\ldots\texttt{10001101}}_{\texttt{IBAN}}\underbrace{\texttt{0011111010010010}}_{\texttt{AMOUNT}}$$

Caveats & Limitations of One-time Pad



$$m = \underbrace{010100000100000101011001}_{\texttt{PAY}}\underbrace{01001001\ldots00110010}_{\texttt{IBAN}}\underbrace{0000000100000100}_{\texttt{AMOUNT (520)}}$$

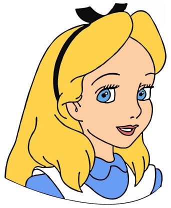
$$c = \underbrace{001101100010101000110101}_{\texttt{PAY}}\underbrace{11010001\ldots10001101}_{\texttt{IBAN}}\underbrace{1011111010010010}_{\texttt{AMOUNT}}$$

$$\oplus \qquad \ldots 1000000000000000$$

$$c' = \underbrace{001101100010101000110101}_{\texttt{PAY}}\underbrace{11010001\ldots10001101}_{\texttt{IBAN}}\underbrace{0011111010010010}_{\texttt{AMOUNT}}$$

$$m' = \underbrace{010100000100000101011001}_{\texttt{PAY}}\underbrace{01001001\ldots00110010}_{\texttt{IBAN}}\underbrace{1000000100000100}_{\texttt{AMOUNT (33028)}}$$

Caveats & Limitations of One-time Pad



$$m = \underbrace{010100000100000101011001}_{\texttt{PAY}}\,\underbrace{01001001\ldots00110010}_{\texttt{IBAN}}\,\underbrace{0000000100000100}_{\texttt{AMOUNT (520)}}$$

$$c = \underbrace{001101100010101000110101}_{\texttt{PAY}}\,\underbrace{11010001\ldots10001101}_{\texttt{IBAN}}\,1011111010010010$$

$\oplus$ 0000

c' 001 ... 10001101 $\underbrace{\color{red}{0}\color{black}{011111010010010}}_{\texttt{AMOUNT}}$

IBAN

$$\underbrace{010100000100000101011001}_{\texttt{PAY}}\,\underbrace{01001001\ldots00110010}_{\texttt{IBAN}}\,\underbrace{\color{red}{1}\color{black}{000000100000100}}_{\texttt{AMOUNT (}\color{red}{33028}\color{black}{)}}$$

Changes to the ciphertext result in predictable changes to the plaintext

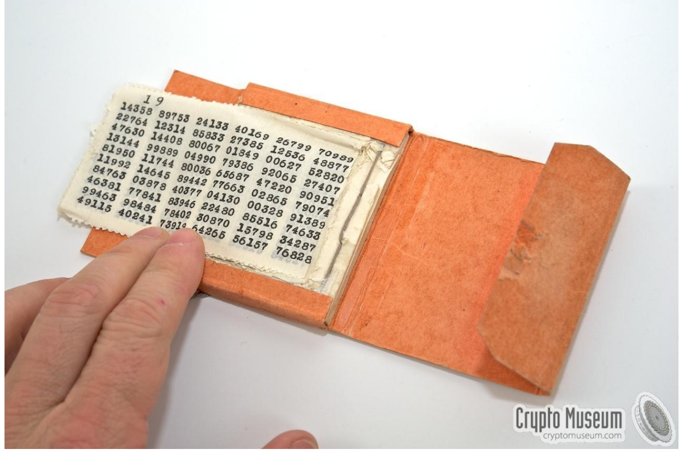
The scheme is **malleable**!

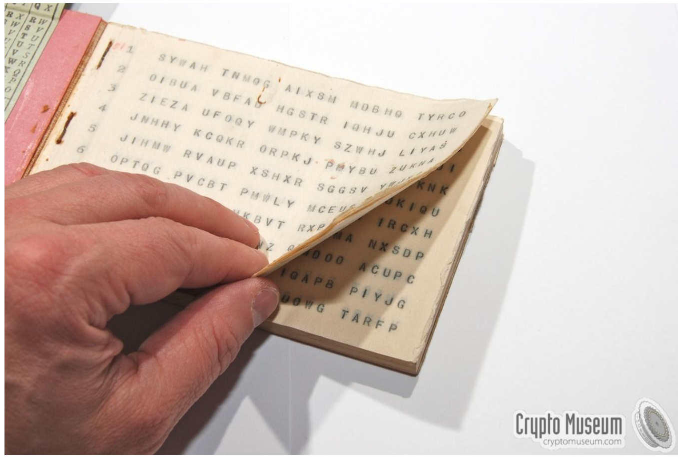
One-time pad in practice

The “red phone”: a symbol of the Moscow–Washington hotline

- Actually consisted of two full-duplex telegraph lines, with teletype terminals at the endpoints
- Text-only: speech can be easily misinterpreted
- Text is encrypted using one-time pad
- Keys were exchanged via the embassies, using trusted couriers with briefcases containing sheets of paper with random characters

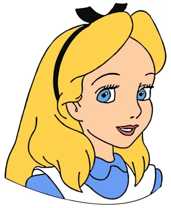
One-time pad in practice





www.cryptomuseum.com

The all-zeros key (Alice's version of OTP)

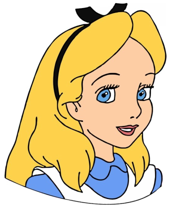


- Alice notices that, when $k = \underbrace{000\dots0}_{\ell \text{ times}}$:

$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

The all-zeros key (Alice's version of OTP)



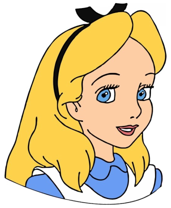
- Alice notices that, when $k = \underbrace{000\ldots0}_{\ell \text{ times}}$:

$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

- How is this compatible with perfect secrecy?

The all-zeros key (Alice's version of OTP)



- Alice notices that, when $k = \underbrace{000\dots0}_{\ell \text{ times}}$:

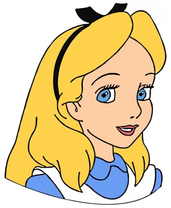
$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

- How is this compatible with perfect secrecy?
- Alice decides to "fix" this problem by redefining $\mathcal{K} = \{0,1\}^\ell \setminus \{000\dots0\}$

Is this modified one-time pad cipher perfectly secret?

The all-zeros key (Alice's version of OTP)



- Alice notices that, when $k = \underbrace{000\ldots0}_{\ell \text{ times}}$:

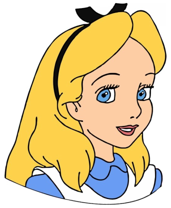
$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

- How is this compatible with perfect secrecy?
- Alice decides to "fix" this problem by redefining $\mathcal{K} = \{0,1\}^\ell \setminus \{000\ldots0\}$

Is this modified one-time pad cipher perfectly secret? **No!**

The all-zeros key (Alice's version of OTP)



- Alice notices that, when $k = \underbrace{000\ldots0}_{\ell \text{ times}}$:

$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

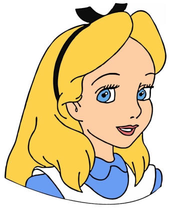
- How is this compatible with perfect secrecy?
- Alice decides to "fix" this problem by redefining $\mathcal{K} = \{0,1\}^\ell \setminus \{000\ldots0\}$

Is this modified one-time pad cipher perfectly secret? **No!**

Using Shannon's definition:

- Pick the uniform distribution of $\mathcal{M}$, any $m \in \mathcal{M}$, and $c = m$

The all-zeros key (Alice's version of OTP)



- Alice notices that, when $k = \underbrace{000\dots0}_{\ell \text{ times}}$:

$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

- How is this compatible with perfect secrecy?
- Alice decides to "fix" this problem by redefining $\mathcal{K} = \{0,1\}^\ell \setminus \{000\dots0\}$

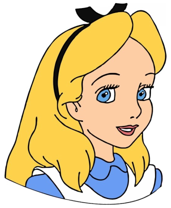
Is this modified one-time pad cipher perfectly secret? **No!**

Using Shannon's definition:

- Pick the uniform distribution of $\mathcal{M}$, any $m \in \mathcal{M}$, and $c = m$

$$\Pr[M = m \mid C = c]$$

The all-zeros key (Alice's version of OTP)



- Alice notices that, when $k = \underbrace{000\dots0}_{\ell \text{ times}}$:

$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

- How is this compatible with perfect secrecy?
- Alice decides to "fix" this problem by redefining $\mathcal{K} = \{0,1\}^\ell \setminus \{000\dots0\}$

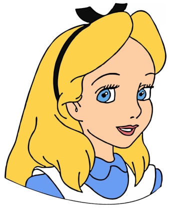
Is this modified one-time pad cipher perfectly secret? **No!**

Using Shannon's definition:

- Pick the uniform distribution of $\mathcal{M}$, any $m \in \mathcal{M}$, and $c = m$

$$\Pr[M = m \mid C = c] = \Pr[C = c \mid M = m] \cdot \frac{\Pr[M=m]}{\Pr[C=c]}$$

The all-zeros key (Alice's version of OTP)



- Alice notices that, when $k = \underbrace{000\ldots0}_{\ell\text{ times}}$:

$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

- How is this compatible with perfect secrecy?
- Alice decides to "fix" this problem by redefining $\mathcal{K} = \{0,1\}^\ell \setminus \{000\ldots0\}$

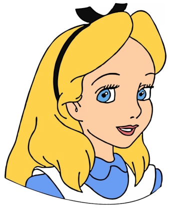
Is this modified one-time pad cipher perfectly secret? **No!**

Using Shannon's definition:

- Pick the uniform distribution of $\mathcal{M}$, any $m \in \mathcal{M}$, and $c = m$

$$\Pr[M = m \mid C = c] = \Pr[C = c \mid M = m] \cdot \frac{\Pr[M=m]}{\Pr[C=c]} = 0$$

The all-zeros key (Alice's version of OTP)



- Alice notices that, when $k = \underbrace{000\ldots0}_{\ell \text{ times}}$:

$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

- How is this compatible with perfect secrecy?
- Alice decides to "fix" this problem by redefining $\mathcal{K} = \{0,1\}^\ell \setminus \{000\ldots0\}$

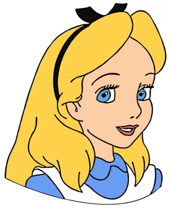
Is this modified one-time pad cipher perfectly secret? **No!**

Using Shannon's definition:

- Pick the uniform distribution of $\mathcal{M}$, any $m \in \mathcal{M}$, and $c = m$

$$\Pr[M = m \mid C = c] = \Pr[C = c \mid M = m] \cdot \tfrac{\Pr[M=m]}{\Pr[C=c]} \quad = 0 \qquad \neq \Pr[M = m]$$

The all-zeros key (Alice's version of OTP)



- Alice notices that, when $k = \underbrace{000\dots0}_{\ell \text{ times}}$:

$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

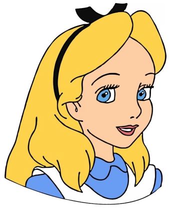
- How is this compatible with perfect secrecy?
- Alice decides to "fix" this problem by redefining $\mathcal{K} = \{0,1\}^\ell \setminus \{000\dots0\}$

Is this modified one-time pad cipher perfectly secret? **No!**

Using the alternative definition:

For any $m' \neq m$ and $c = m$: $\Pr[\mathsf{Enc}_K(m) = c] = \Pr[K = 00\dots0] = 0$

The all-zeros key (Alice's version of OTP)



- Alice notices that, when $k = \underbrace{000\dots0}_{\ell \text{ times}}$:

$$\mathsf{Enc}_k(m) = k \oplus m = m$$

The ciphertext coincides with the plaintext!

- How is this compatible with perfect secrecy?
- Alice decides to "fix" this problem by redefining $\mathcal{K} = \{0,1\}^\ell \setminus \{000\dots0\}$

Is this modified one-time pad cipher perfectly secret? **No!**

Using the alternative definition:

For any $m' \neq m$ and $c = m$:

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[K = 00\dots0] = 0$$

$$\Pr[\mathsf{Enc}_K(m') = c] = \Pr[K = m' \oplus c] \neq 0$$

Limitations of Perfect Secrecy

The Vernam cipher is perfectly secret, but. . .

Limitations of Perfect Secrecy

The Vernam cipher is perfectly secret, but...

...keys are long and difficult to share/store

Limitations of Perfect Secrecy

The Vernam cipher is perfectly secret, but...

...keys are long and difficult to share/store

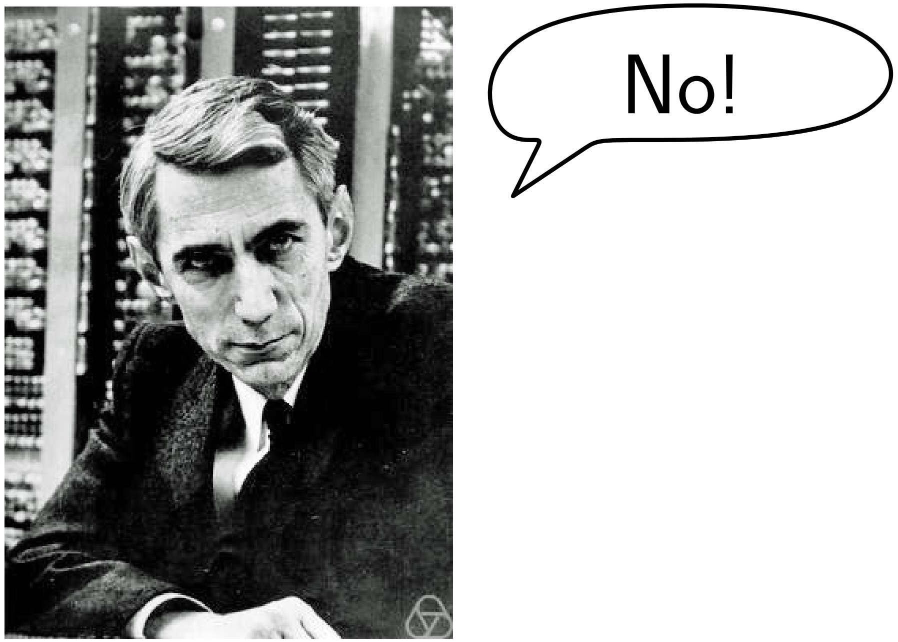
Is there a perfectly secure cipher that uses short keys?

Limitations of Perfect Secrecy

The Vernam cipher is perfectly secret, but. . .

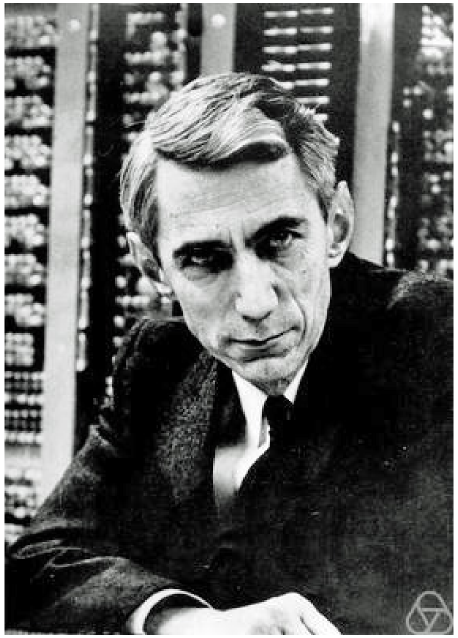
. . . keys are long and difficult to share/store

Is there a perfectly secure cipher that uses short keys?



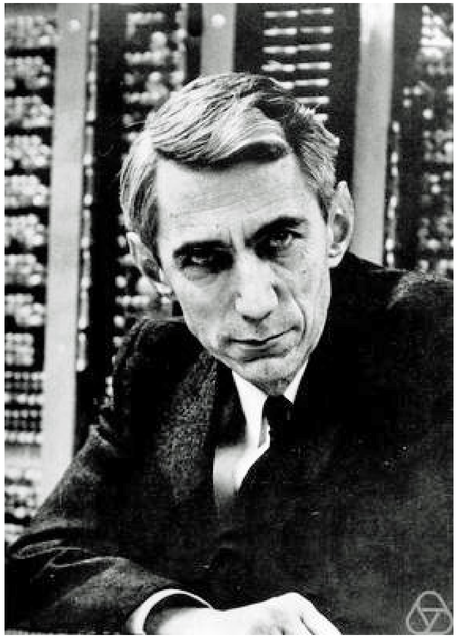
Limitations of Perfect Secrecy

Theorem: *If* (Gen, Enc, Dec) *is a perfectly secret encryption scheme with message space* $\mathcal{M}$ *and key space* $\mathcal{K}$*, then* $|\mathcal{K}| \geq |\mathcal{M}|$



Limitations of Perfect Secrecy

Theorem: *If* (Gen, Enc, Dec) *is a perfectly secret encryption scheme with message space* $\mathcal{M}$ *and key space* $\mathcal{K}$*, then* $|\mathcal{K}| \geq |\mathcal{M}|$



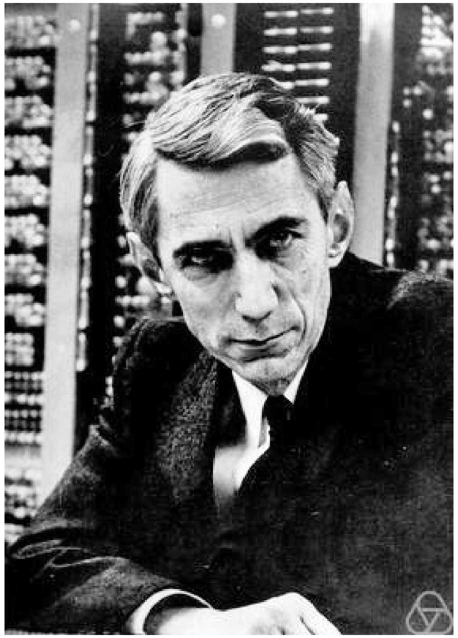
Proof:

We prove the contrapositive statement:

If $|\mathcal{K}| < |\mathcal{M}|$ then the encryption scheme is not perfectly secret.

Limitations of Perfect Secrecy

Theorem: *If* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *is a perfectly secret encryption scheme with message space* $\mathcal{M}$ *and key space* $\mathcal{K}$*, then* $|\mathcal{K}| \geq |\mathcal{M}|$



Proof:

We prove the contrapositive statement:

If $|\mathcal{K}| < |\mathcal{M}|$ then the encryption scheme is not perfectly secret.

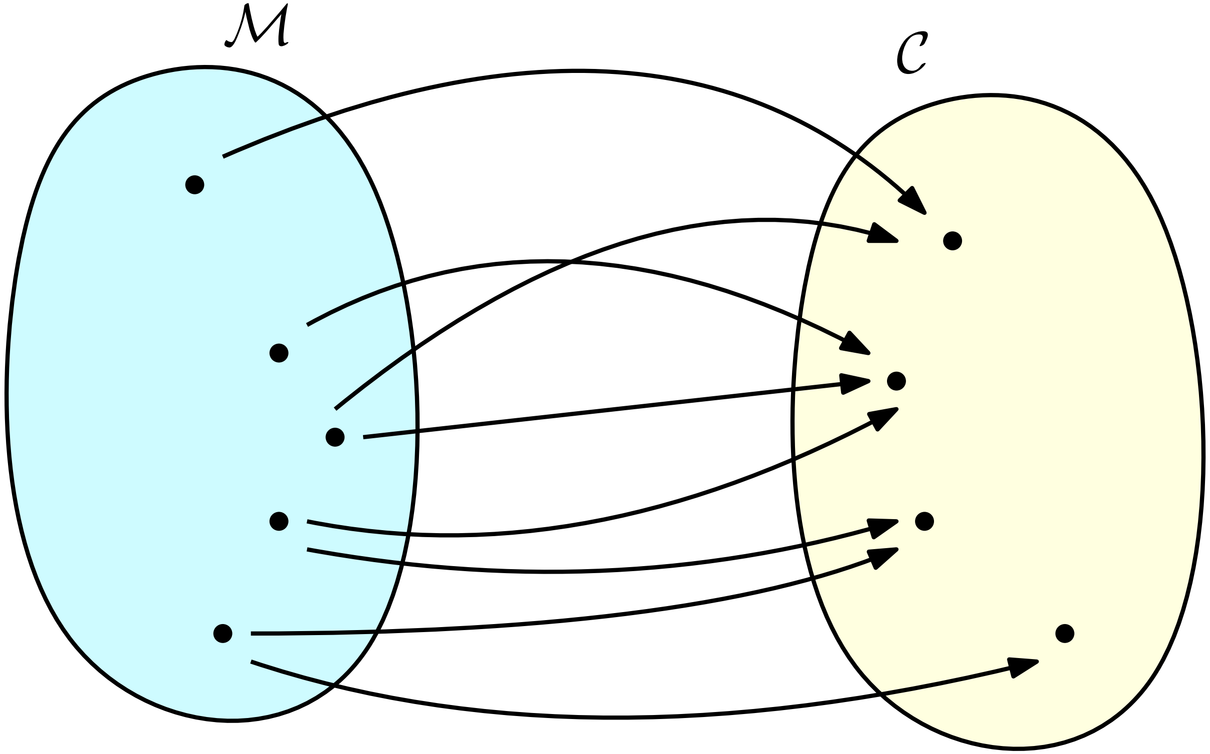
In particular, we argue that there must exist some m' for which:

$$\Pr[M = m'] \neq \Pr[\mathcal{M} = m' \mid C = c]$$

Limitations of Perfect Secrecy

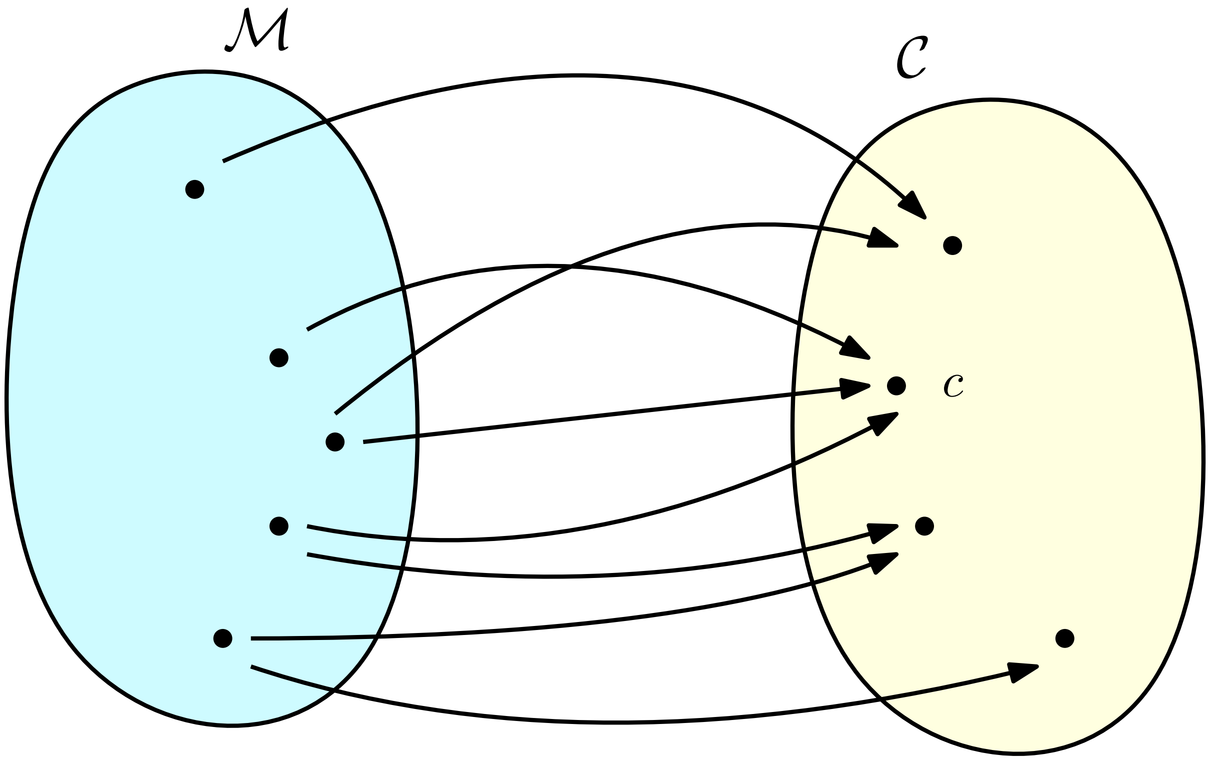
$m \;\bullet \longrightarrow \bullet\; c$

denotes that the plaintext m can
be encrypted to the ciphertext c
(using a suitable key)



Limitations of Perfect Secrecy

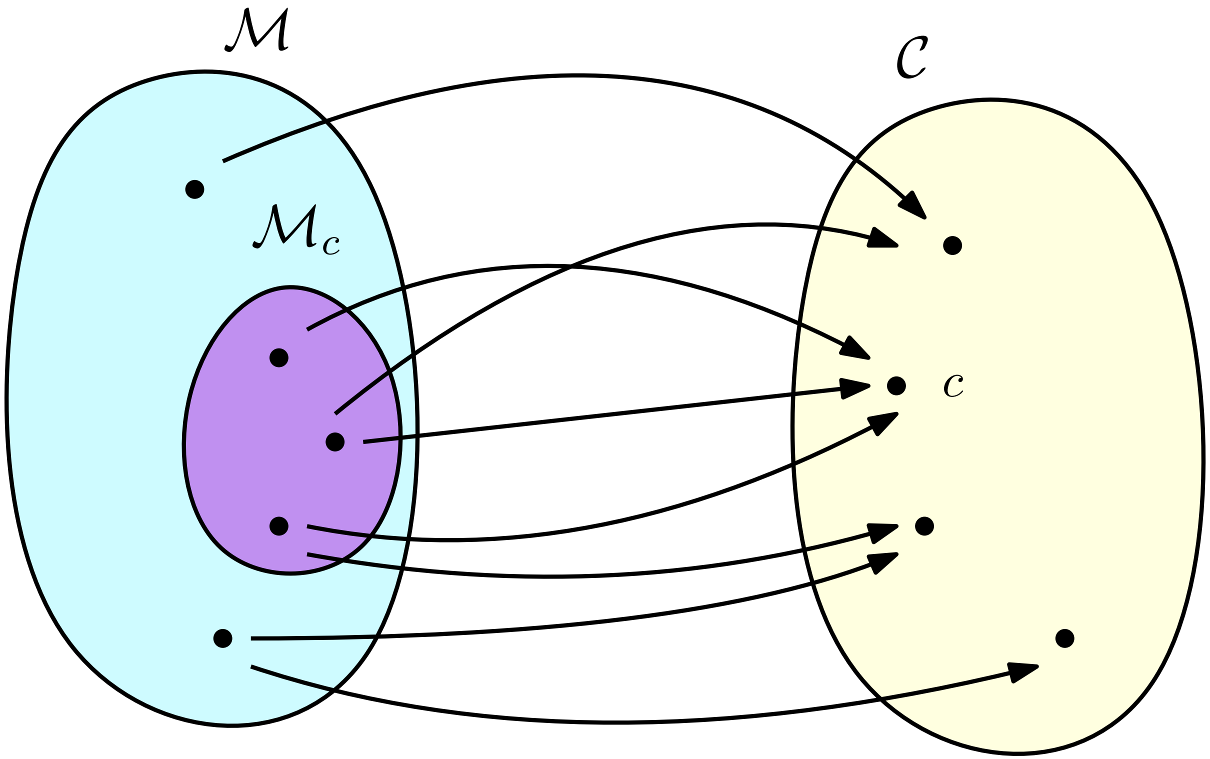
Consider the uniform distribution over $\mathcal{M}$ and let c be a ciphertext that occurs with positive probability



Limitations of Perfect Secrecy

Consider the uniform distribution over $\mathcal{M}$ and let c be a ciphertext that occurs with positive probability

Let $\mathcal{M}_c$ denote all messages $m \in \mathcal{M}$ such that $m = \mathsf{Dec}_k(c)$ for some $k \in \mathcal{K}$



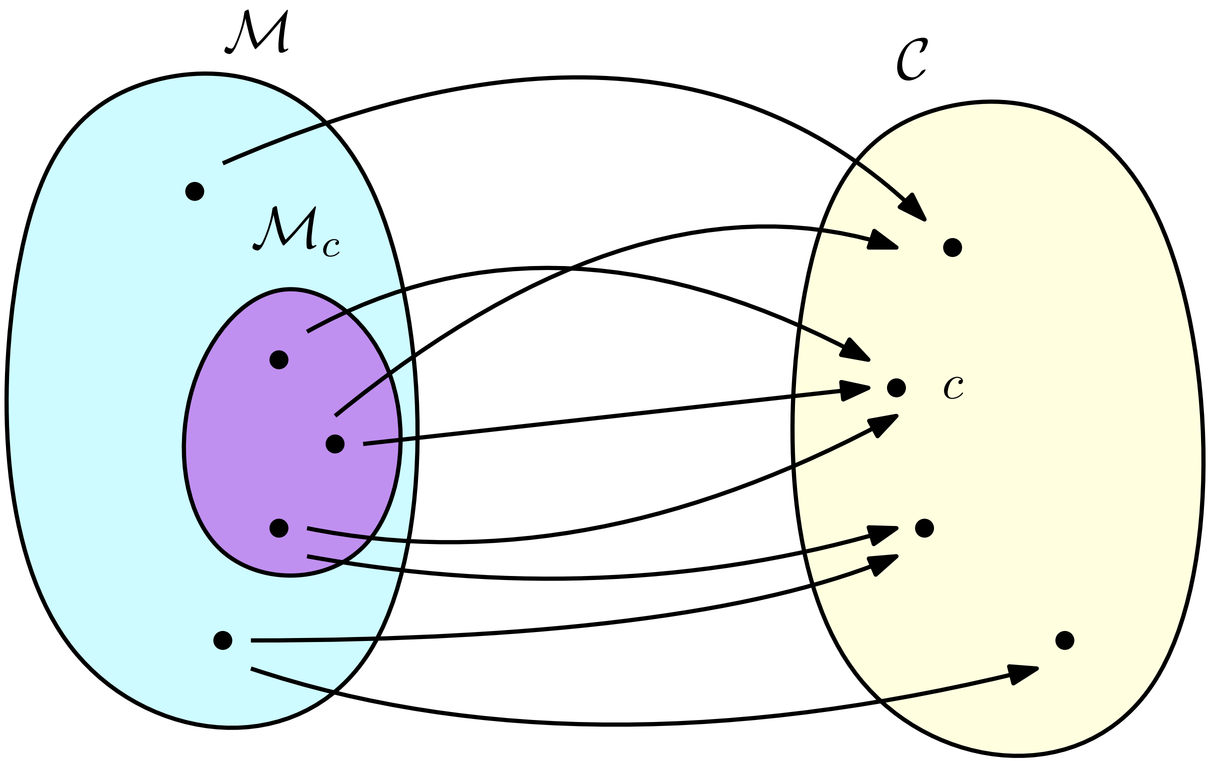
Limitations of Perfect Secrecy

Consider the uniform distribution over $\mathcal{M}$ and let c be a ciphertext that occurs with positive probability

Let $\mathcal{M}_c$ denote all messages $m \in \mathcal{M}$ such that $m = \mathsf{Dec}_k(c)$ for some $k \in \mathcal{K}$

Since Dec is a deterministic algorithm:

$$|\mathcal{M}_c| \leq |\mathcal{K}| < |\mathcal{M}|$$
$$\Downarrow$$
$$\mathcal{M} \setminus \mathcal{M}_c \neq \emptyset$$



Limitations of Perfect Secrecy

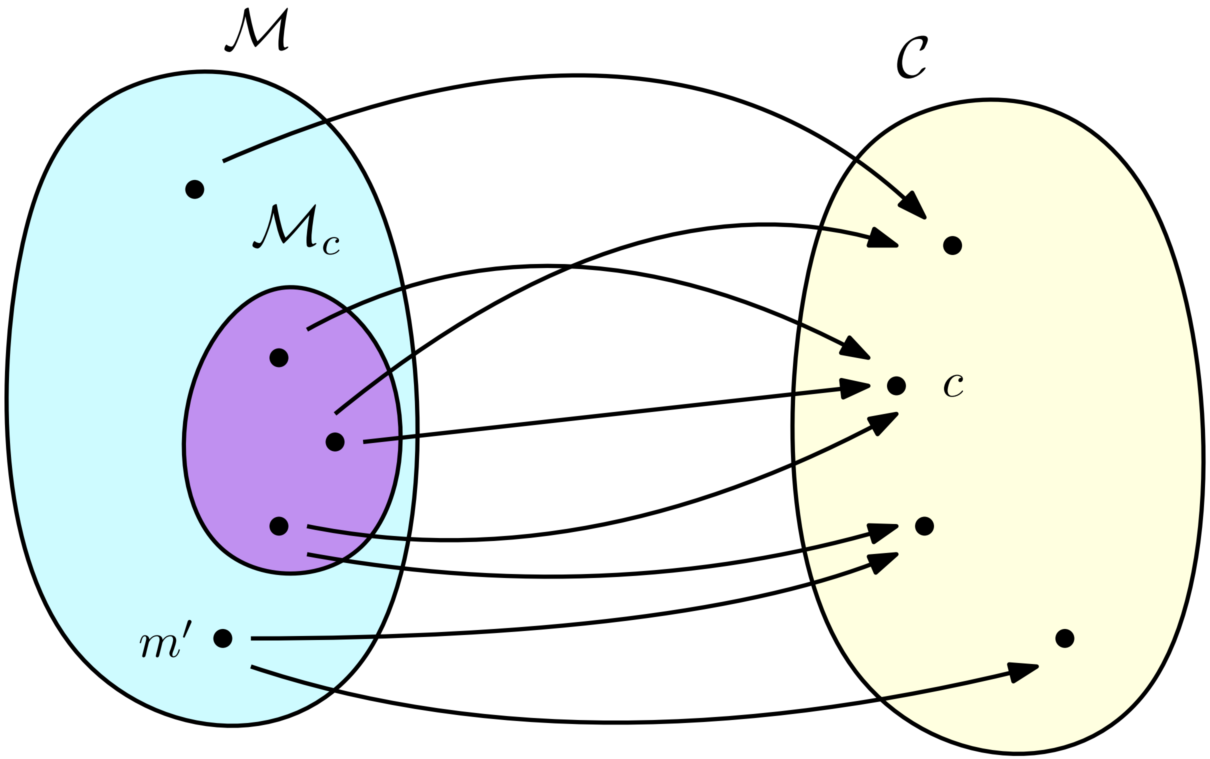
Consider the uniform distribution over $\mathcal{M}$ and let c be a ciphertext that occurs with positive probability

Let $\mathcal{M}_c$ denote all messages $m \in \mathcal{M}$ such that $m = \mathsf{Dec}_k(c)$ for some $k \in \mathcal{K}$

Since Dec is a deterministic algorithm:

$$|\mathcal{M}_c| \leq |\mathcal{K}| < |\mathcal{M}|$$
$$\Downarrow$$
$$\mathcal{M} \setminus \mathcal{M}_c \neq \emptyset$$

Pick any $m' \in \mathcal{M} \setminus \mathcal{M}_c$



Limitations of Perfect Secrecy

Consider the uniform distribution over $\mathcal{M}$ and let c be a ciphertext that occurs with positive probability

Let $\mathcal{M}_c$ denote all messages $m \in \mathcal{M}$ such that $m = \mathsf{Dec}_k(c)$ for some $k \in \mathcal{K}$

Since Dec is a deterministic algorithm:

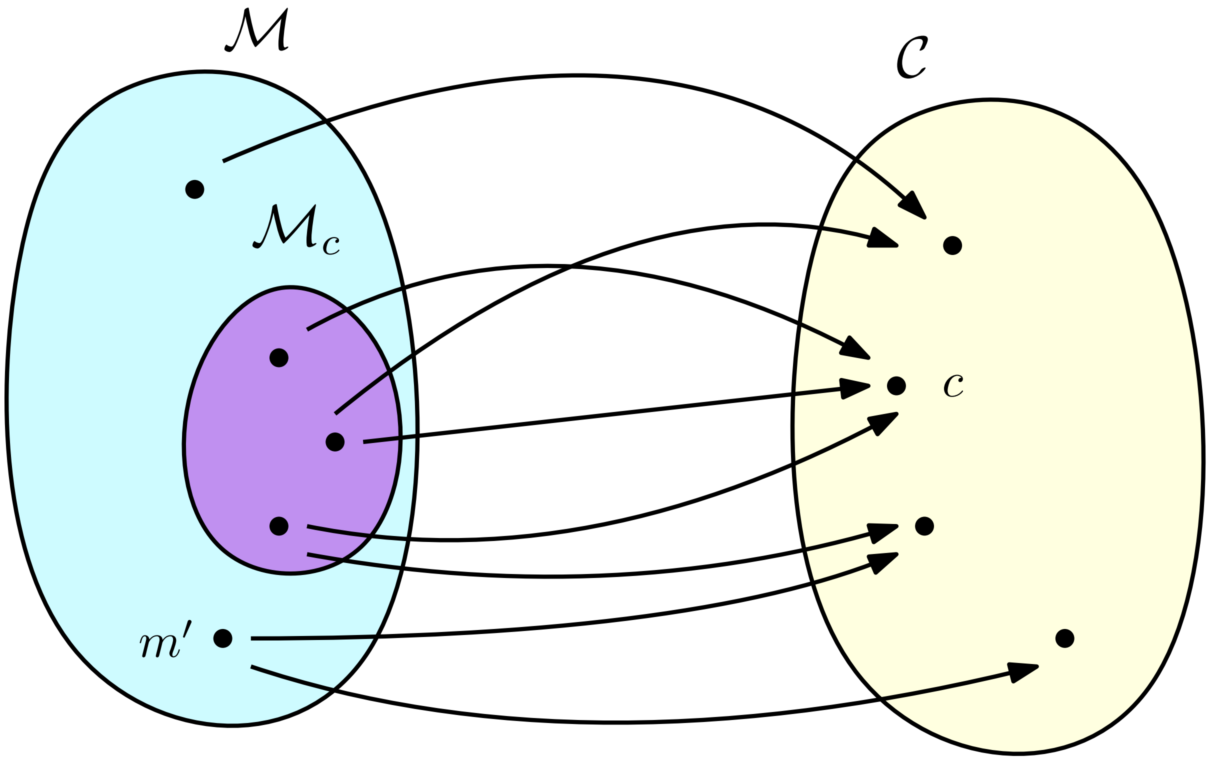
$$|\mathcal{M}_c| \leq |\mathcal{K}| < |\mathcal{M}|$$

$$\Downarrow$$

$$\mathcal{M} \setminus \mathcal{M}_c \neq \emptyset$$

Pick any $m' \in \mathcal{M} \setminus \mathcal{M}_c$

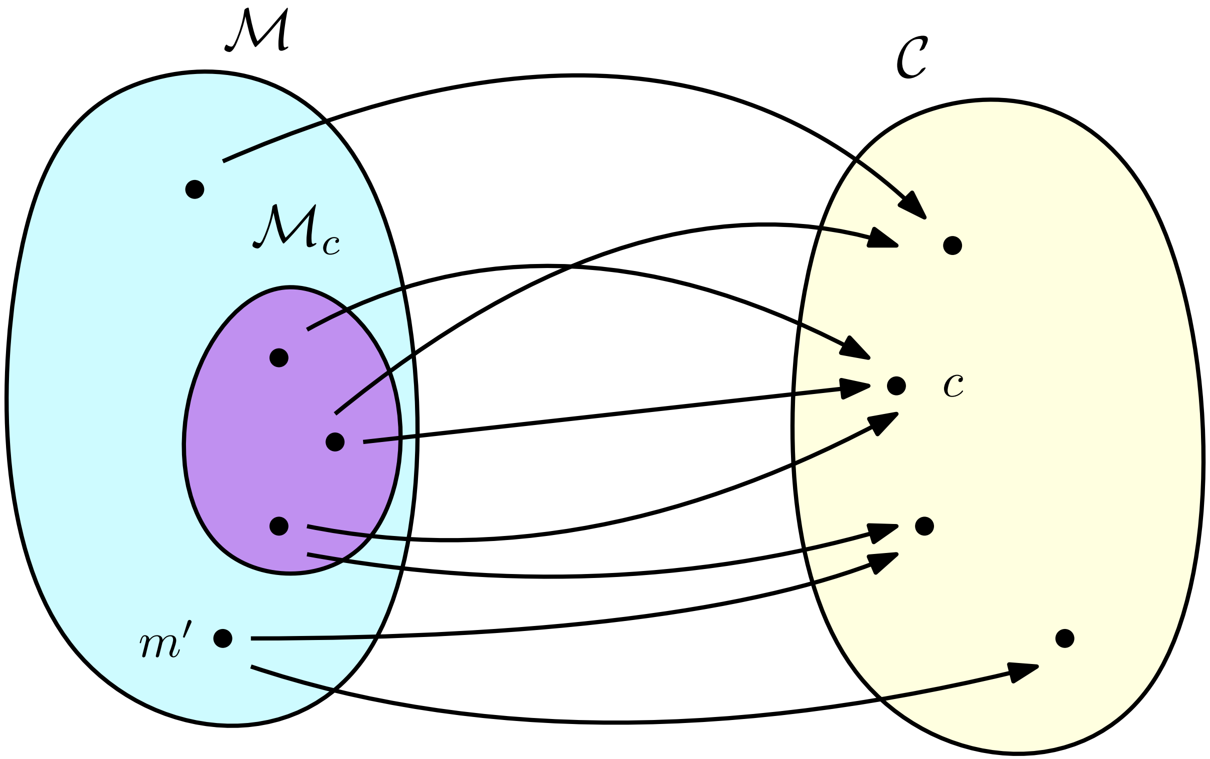
- $\Pr[M = m'] > 0$



Limitations of Perfect Secrecy

Consider the uniform distribution over $\mathcal{M}$ and let c be a ciphertext that occurs with positive probability

Let $\mathcal{M}_c$ denote all messages $m \in \mathcal{M}$ such that $m = \mathsf{Dec}_k(c)$ for some $k \in \mathcal{K}$



Since Dec is a deterministic algorithm:

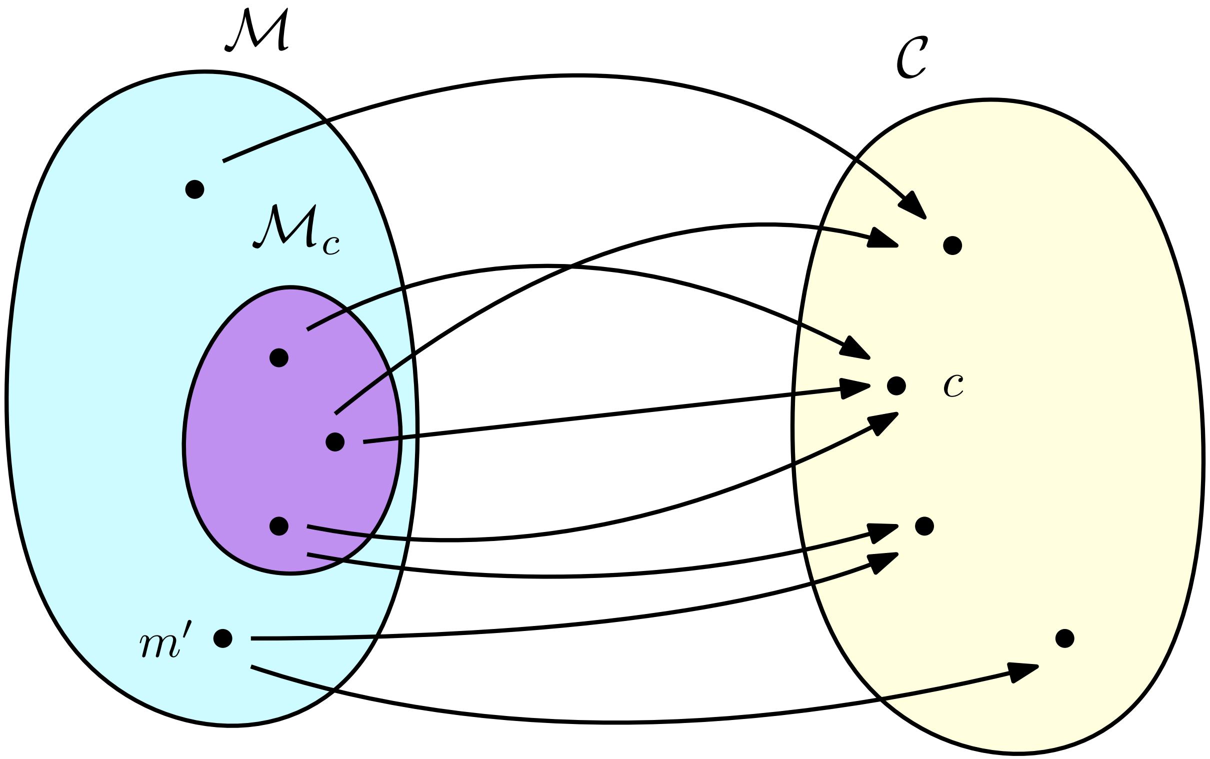
$$|\mathcal{M}_c| \leq |\mathcal{K}| < |\mathcal{M}|$$
$$\Downarrow$$
$$\mathcal{M} \setminus \mathcal{M}_c \neq \emptyset$$

Pick any $m' \in \mathcal{M} \setminus \mathcal{M}_c$

- $\Pr[M = m'] > 0$
- $\Pr[M = m' \mid C = c] = 0$

Limitations of Perfect Secrecy

Consider the uniform distribution over $\mathcal{M}$ and let c be a ciphertext that occurs with positive probability



Let $\mathcal{M}_c$ denote all messages $m \in \mathcal{M}$ such that $m = \mathsf{Dec}_k(c)$ for some $k \in \mathcal{K}$

Since Dec is a deterministic algorithm:

$$|\mathcal{M}_c| \le |\mathcal{K}| < |\mathcal{M}| \\ \Downarrow \\ \mathcal{M} \setminus \mathcal{M}_c \neq \emptyset$$

Pick any $m' \in \mathcal{M} \setminus \mathcal{M}_c$

$$\left.\begin{array}{l} \bullet\ \Pr[M = m'] > 0 \\ \bullet\ \Pr[M = m' \mid C = c] = 0 \end{array}\right\} \implies \Pr[M = m'] \neq \Pr[\mathcal{M} = m' \mid C = c]$$

$\square$

Limitations of Perfect Secrecy

Theorem: *If* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *is a perfectly secret encryption scheme with message space* $\mathcal{M}$ *and key space* $\mathcal{K}$, *then* $|\mathcal{K}| \geq |\mathcal{M}|$

Corollary: *Any perfectly secret encryption scheme with* $\mathcal{M} = \{0,1\}^{\ell}$ *and* $\mathcal{K} \subseteq \{0,1\}^{*}$ *is such that* $\max_{k \in \mathcal{K}} |k| \geq \ell$, *where* $|k|$ *denotes the number of bits of* k

Limitations of Perfect Secrecy

Theorem: *If* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *is a perfectly secret encryption scheme with message space* $\mathcal{M}$ *and key space* $\mathcal{K}$*, then* $|\mathcal{K}| \geq |\mathcal{M}|$

Corollary: *Any perfectly secret encryption scheme with* $\mathcal{M} = \{0,1\}^\ell$ *and* $\mathcal{K} \subseteq \{0,1\}^*$ *is such that* $\max_{k \in \mathcal{K}} |k| \geq \ell$*, where* $|k|$ *denotes the number of bits of* k

Inf. If an encryption scheme is perfectly secret and is able to encrypt any message of length ℓ (over the binary alphabet) then it must require the use of at least one key with length at least ℓ.

Limitations of Perfect Secrecy

Theorem: *If* (Gen, Enc, Dec) *is a perfectly secret encryption scheme with message space* $\mathcal{M}$ *and key space* $\mathcal{K}$*, then* $|\mathcal{K}| \geq |\mathcal{M}|$

Corollary: *Any perfectly secret encryption scheme with* $\mathcal{M} = \{0,1\}^\ell$ *and* $\mathcal{K} \subseteq \{0,1\}^*$ *is such that* $\max_{k \in \mathcal{K}} |k| \geq \ell$*, where* $|k|$ *denotes the number of bits of* k

Inf. If an encryption scheme is perfectly secret and is able to encrypt any message of length ℓ (over the binary alphabet) then it must require the use of at least one key with length at least ℓ.

Proof:

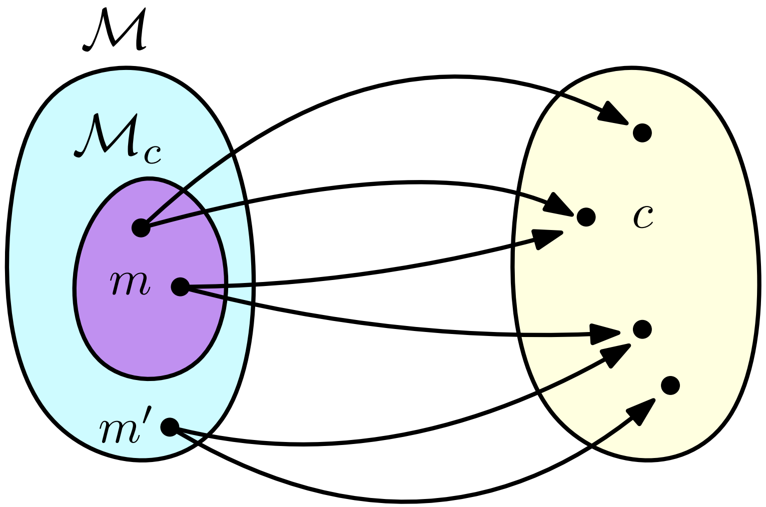
If all keys have length at most $\ell' < \ell$ then the encryption scheme cannot be perfectly secret. Indeed:

$$|\mathcal{K}| \leq \sum_{i=0}^{\ell'} |\{0,1\}^i| = \sum_{i=0}^{\ell'} 2^i = 2^{\ell'+1} - 1 \leq 2^\ell - 1 < 2^\ell = |\mathcal{M}| \qquad \square$$

A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)

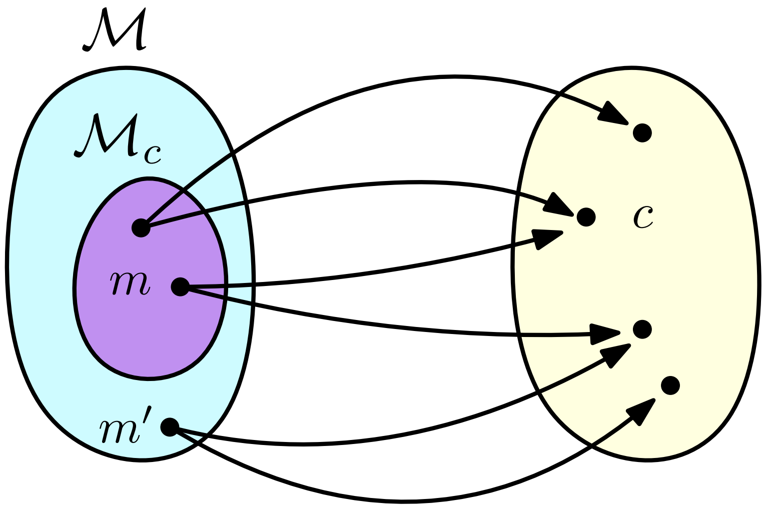


A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)

Distinguisher $\mathcal{A}$:



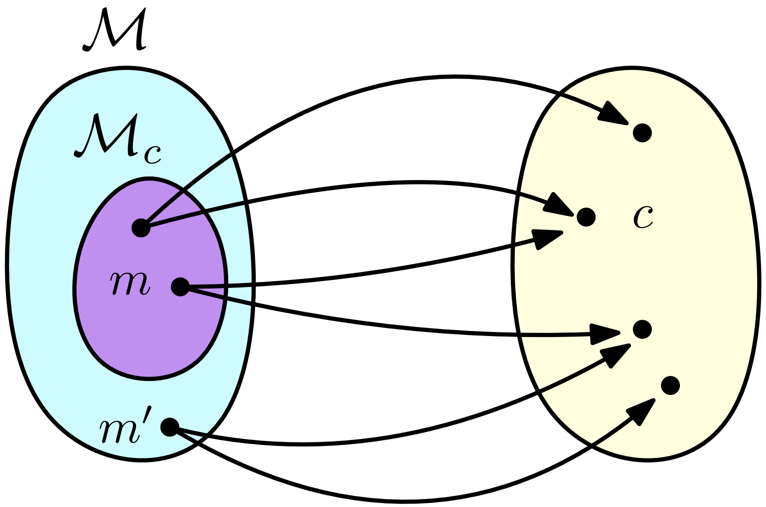
A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)

Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$



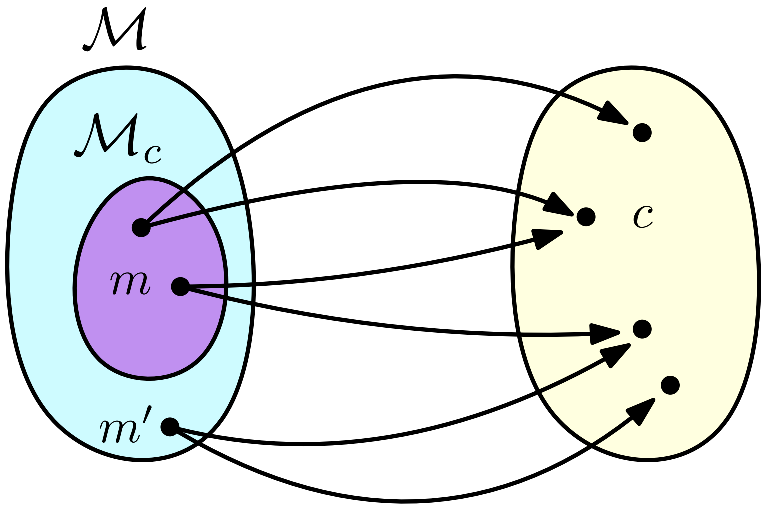
A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)

Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$



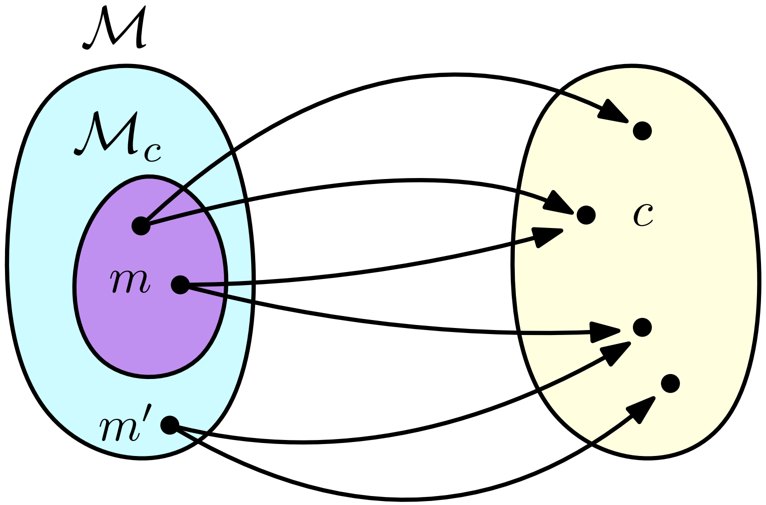
A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)

Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0, 1\}$



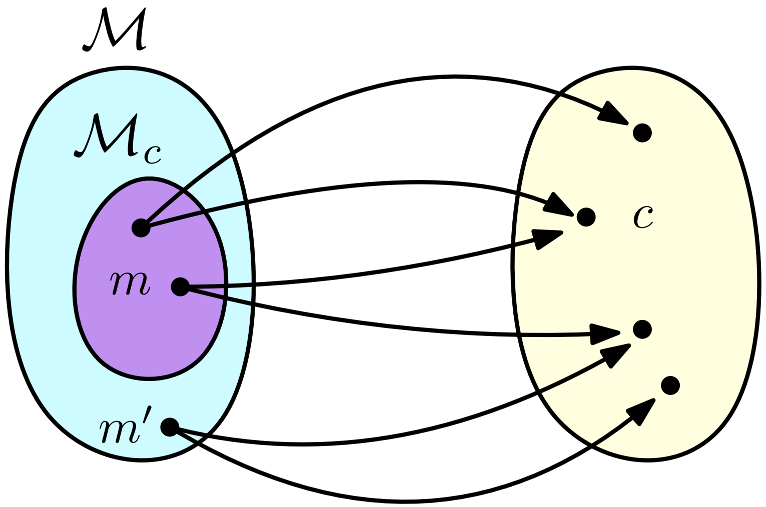
A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)

Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0, 1\}$



$\Pr[b' = 0 \mid b = 0] =$

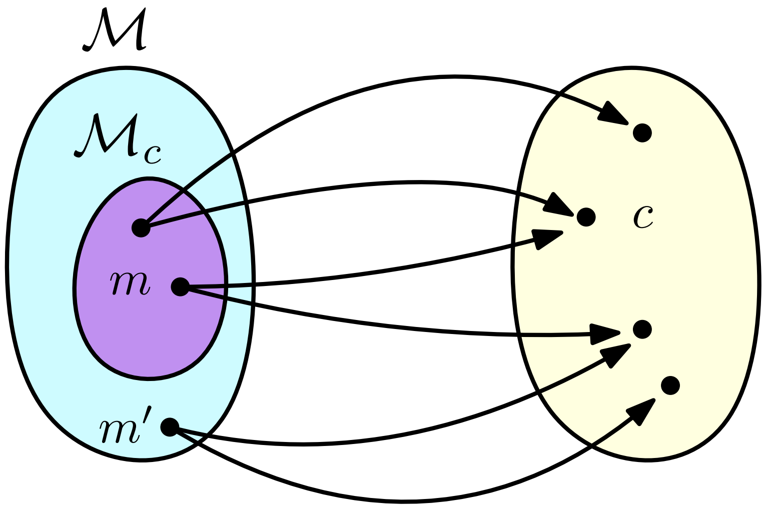
A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)

Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0, 1\}$

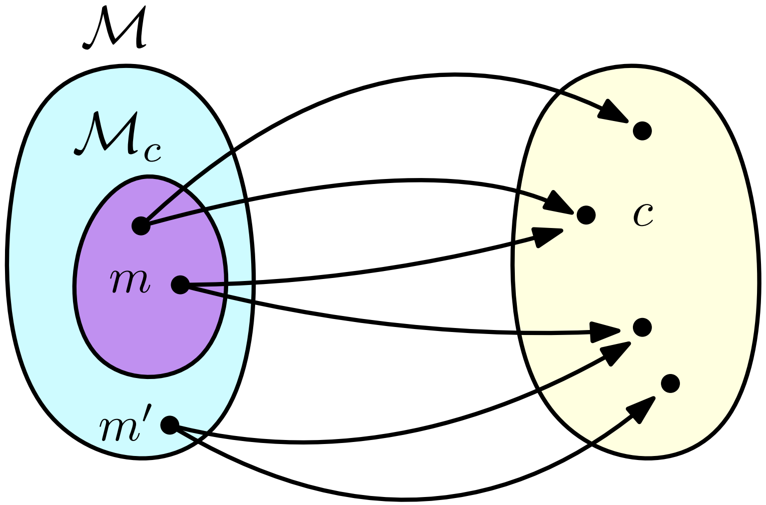


$$\begin{aligned}\Pr[b' = 0 \mid b = 0] = \quad & \Pr[b' = 0 \mid \mathsf{Enc}_K(m_0) = c]\,\Pr[\mathsf{Enc}_K(m_0) = c] \\ & + \Pr[b' = 0 \mid \mathsf{Enc}_K(m_0) \neq c]\,\Pr[\mathsf{Enc}_K(m_0) \neq c]\end{aligned}$$

A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)



Distinguisher $\mathcal{A}$:

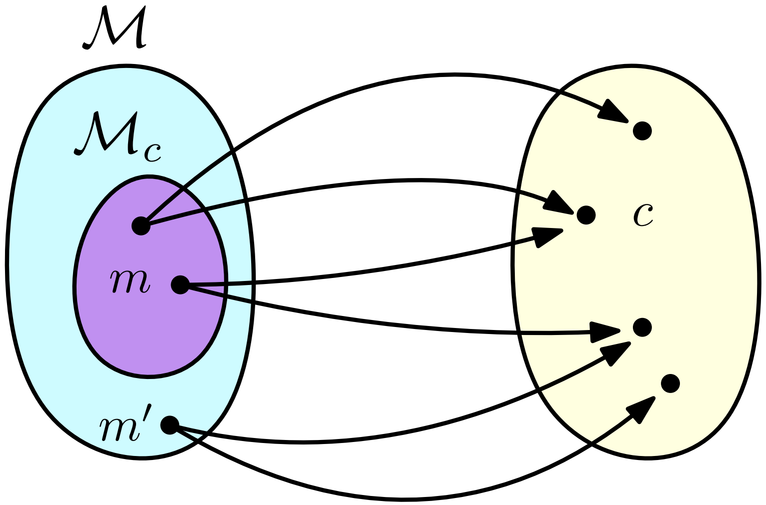
- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0,1\}$

$$
\begin{aligned}
\Pr[b' = 0 \mid b = 0] = {} & 1 \cdot \varepsilon \\
& + \Pr[b' = 0 \mid \mathsf{Enc}_K(m_0) \neq c] \Pr[\mathsf{Enc}_K(m_0) \neq c]
\end{aligned}
$$

A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)



Distinguisher $\mathcal{A}$:

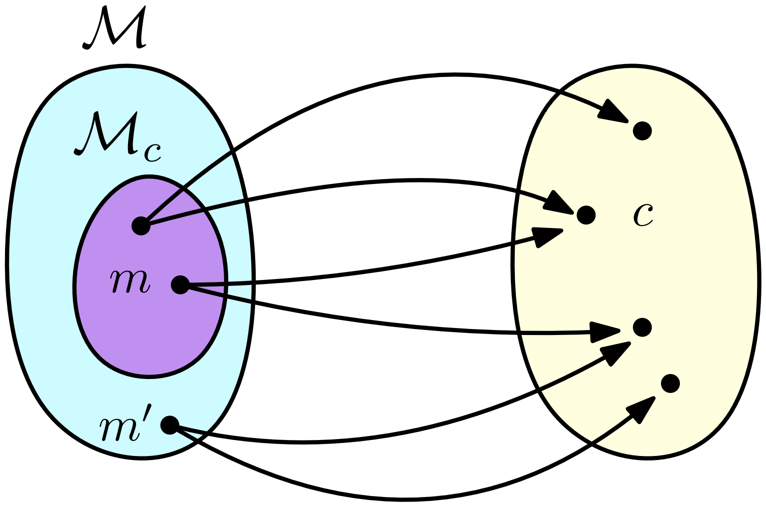
- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0, 1\}$

$$\Pr[b' = 0 \mid b = 0] = 1 \cdot \varepsilon + \tfrac{1}{2} \cdot (1 - \varepsilon)$$

A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)



Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0, 1\}$

$\Pr[b' = 0 \mid b = 0] = \frac{1}{2} + \frac{\varepsilon}{2}$

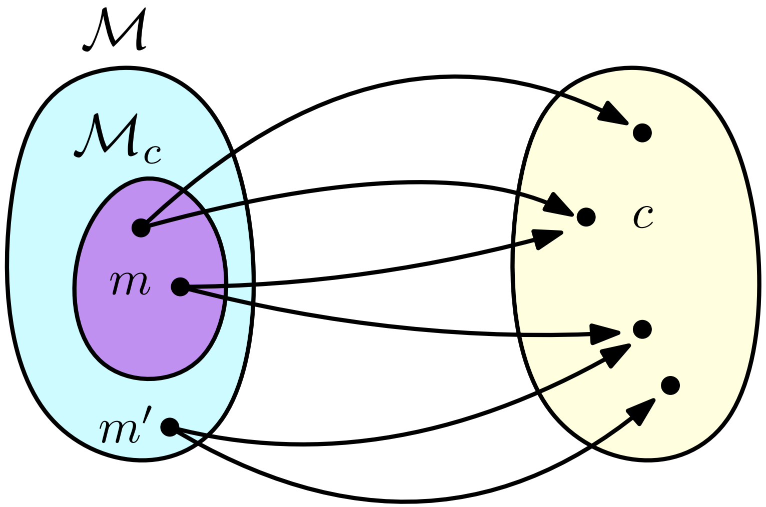
A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)

Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0, 1\}$



$\Pr[b' = 0 \mid b = 0] = \frac{1}{2} + \frac{\varepsilon}{2}$

$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$

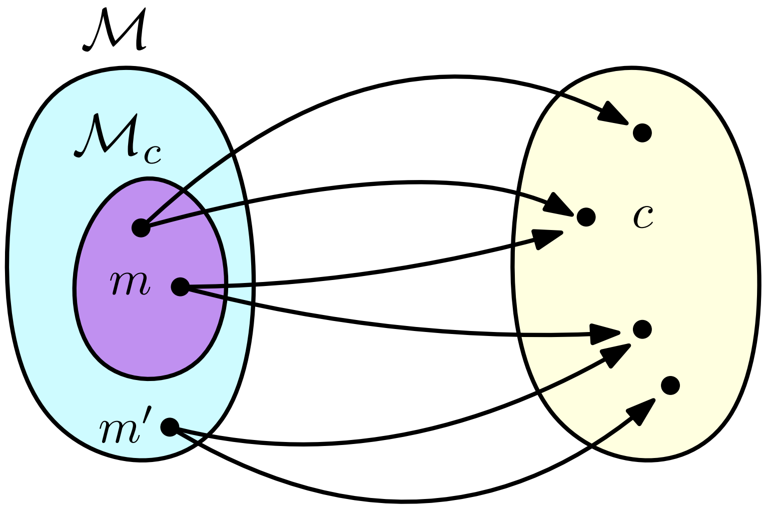
A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)

Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0, 1\}$



$$\Pr[b' = 0 \mid b = 0] = \frac{1}{2} + \frac{\varepsilon}{2}$$

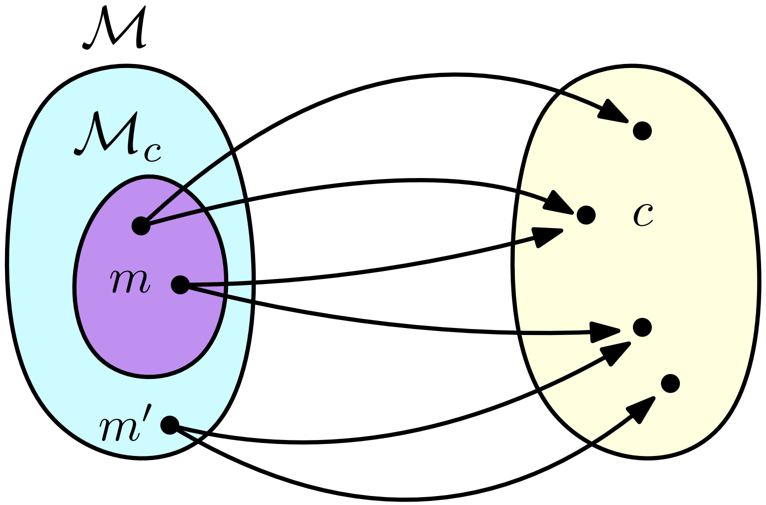
$$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \Pr[b' = 0 \mid b = 0]\Pr[b = 0] + \Pr[b' = 1 \mid b = 1]\Pr[b = 1]$$

A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)



Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0, 1\}$

$$\Pr[b' = 0 \mid b = 0] = \frac{1}{2} + \frac{\varepsilon}{2}$$

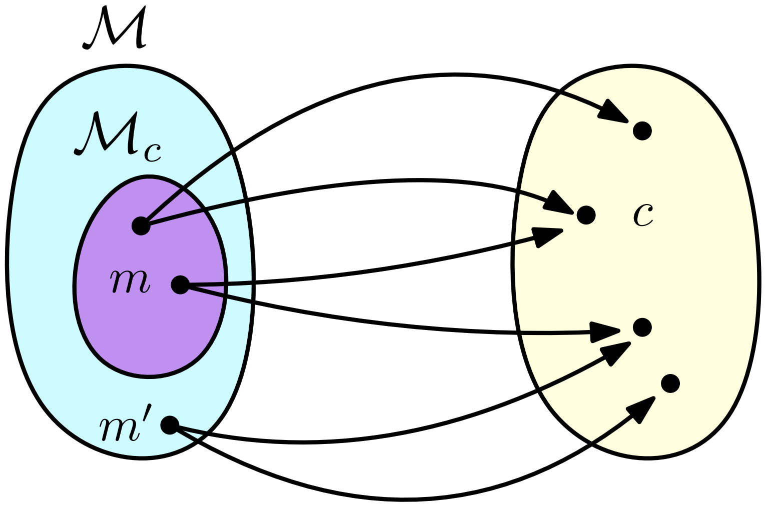
$$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = (\frac{1}{2} + \frac{\epsilon}{2}) \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2}$$

A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)



Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0, 1\}$

$$\Pr[b' = 0 \mid b = 0] = \frac{1}{2} + \frac{\varepsilon}{2}$$

$$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$$

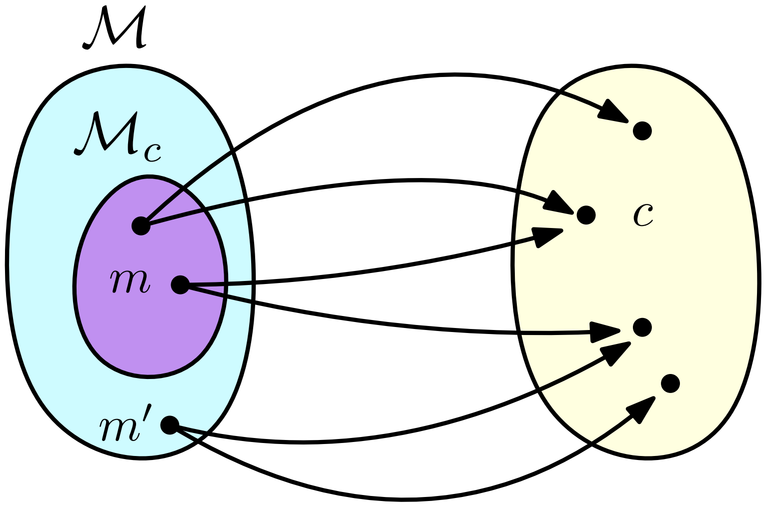
$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = (\frac{1}{2} + \frac{\epsilon}{2}) \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2} + \frac{\varepsilon}{4}$$

Advantage!

A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)



Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - Output $b' = 0$ if $\bar{c} = c$
  - Otherwise output a random guess $b' \in \{0, 1\}$

$$\Pr[b' = 0 \mid b = 0] = \frac{1}{2} + \frac{\varepsilon}{2}$$

$$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$$

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = (\frac{1}{2} + \frac{\epsilon}{2}) \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2} + \frac{\varepsilon}{4}$$

Advantage!

Note: ε can be tiny!

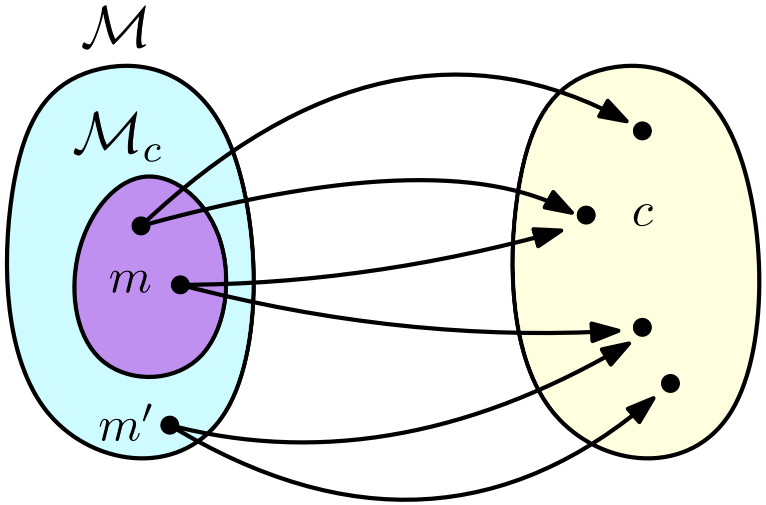
A concrete attack

The proof of the theorem shows that there are some $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$ such that:

- $m \in \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m) = c] = \varepsilon$ for some $\varepsilon > 0$)
- $m' \notin \mathcal{M}_c$ (i.e., $\Pr[\mathsf{Enc}_K(m') = c] = 0$)

Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
    - Output $b' = 0$ if $\bar{c} = c$
    - Otherwise output a random guess $b' \in \{0, 1\}$



$$\Pr[b' = 0 \mid b = 0] = \frac{1}{2} + \frac{\varepsilon}{2}$$

$$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$$

Running time?

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \left(\frac{1}{2} + \frac{\epsilon}{2}\right) \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2} + \frac{\varepsilon}{4}$$

Advantage!

Note: ε can be tiny!

Another concrete attack

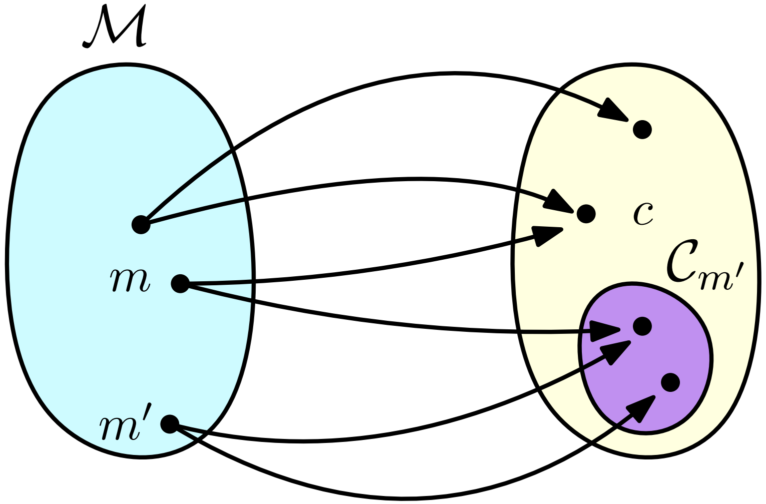
Let $\mathcal{C}_{m'}$ be the set of all ciphertexts c' such that $\mathsf{Dec}_k(c') = m'$ for some $k \in \mathcal{K}$

Another concrete attack

Let $\mathcal{C}_{m'}$ be the set of all ciphertexts c' such that $\mathsf{Dec}_k(c') = m'$ for some $k \in \mathcal{K}$

The proof of the theorem shows that there are $m, m' \in \mathcal{M}$ such that:

There is a ciphertext c that can be obtained by encrypting m but cannot be obtained by encrypting m'



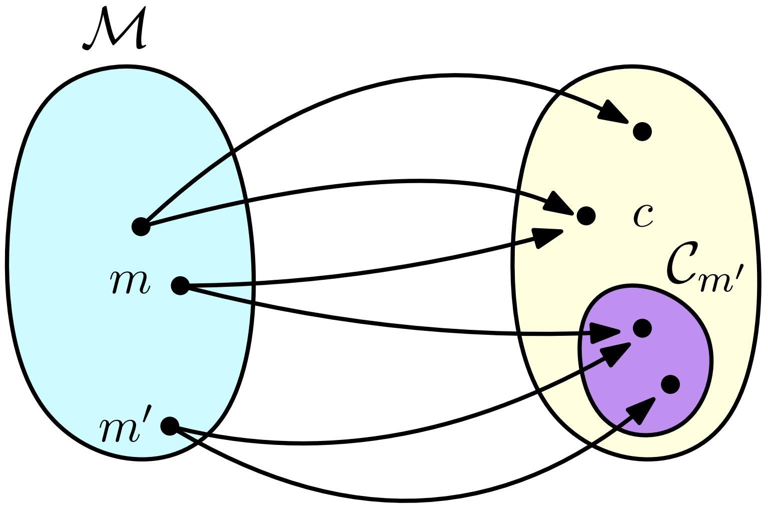
Another concrete attack

Let $\mathcal{C}_{m'}$ be the set of all ciphertexts c' such that $\mathsf{Dec}_k(c') = m'$ for some $k \in \mathcal{K}$

The proof of the theorem shows that there are $m, m' \in \mathcal{M}$ such that:

There is a ciphertext c that can be obtained by encrypting m but cannot be obtained by encrypting m'

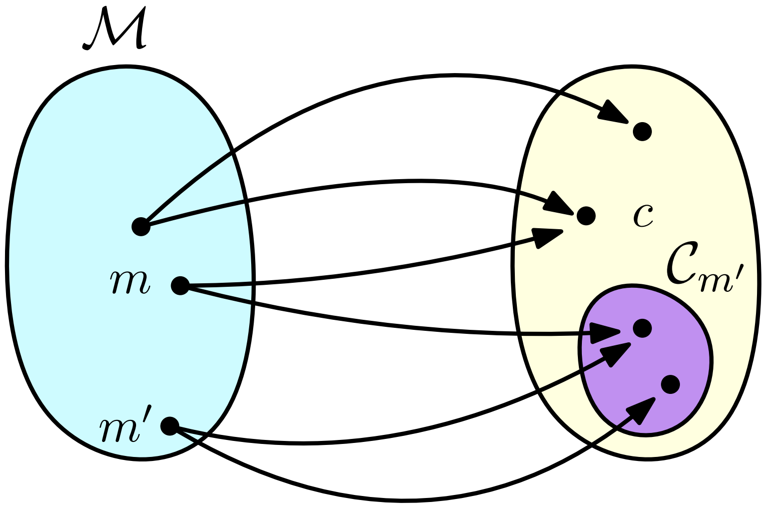
$$\Pr[\mathsf{Enc}_K(m) \in \mathcal{C}_{m'}] = 1 - \varepsilon \text{ for some } \varepsilon > 0$$



Another concrete attack

Let $\mathcal{C}_{m'}$ be the set of all ciphertexts c' such that $\mathsf{Dec}_k(c') = m'$ for some $k \in \mathcal{K}$

The proof of the theorem shows that there are $m, m' \in \mathcal{M}$ such that:



There is a ciphertext c that can be obtained by encrypting m but cannot be obtained by encrypting m'

$$\Pr[\mathsf{Enc}_K(m) \in \mathcal{C}_{m'}] = 1 - \varepsilon \text{ for some } \varepsilon > 0$$

Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - If $\bar{c} \in \mathcal{C}_{m'}$, output a random guess $b' \in \{0,1\}$
  - Otherwise output $b' = 0$

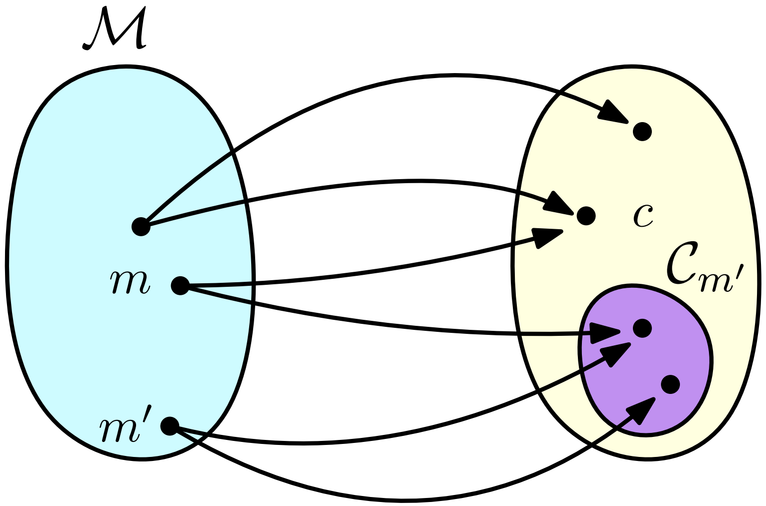
Another concrete attack

Let $\mathcal{C}_{m'}$ be the set of all ciphertexts c' such that $\mathsf{Dec}_k(c') = m'$ for some $k \in \mathcal{K}$

The proof of the theorem shows that there are $m, m' \in \mathcal{M}$ such that:

There is a ciphertext c that can be obtained by encrypting m but cannot be obtained by encrypting m'

$$\Pr[\mathsf{Enc}_K(m) \in \mathcal{C}_{m'}] = 1 - \varepsilon \text{ for some } \varepsilon > 0$$



Running time?

Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - If $\bar{c} \in \mathcal{C}_{m'}$, output a random guess $b' \in \{0,1\}$
  - Otherwise output $b' = 0$

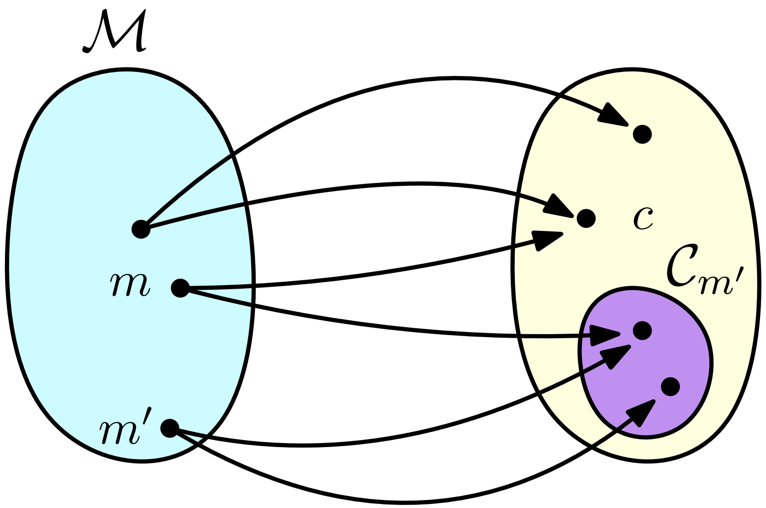
Another concrete attack

Let $\mathcal{C}_{m'}$ be the set of all ciphertexts c' such that $\mathsf{Dec}_k(c') = m'$ for some $k \in \mathcal{K}$

The proof of the theorem shows that there are $m, m' \in \mathcal{M}$ such that:

There is a ciphertext c that can be obtained by encrypting m but cannot be obtained by encrypting m'

$$\Pr[\mathsf{Enc}_K(m) \in \mathcal{C}_{m'}] = 1 - \varepsilon \text{ for some } \varepsilon > 0$$



Distinguisher $\mathcal{A}$:

- Output $m_0 = m$ and $m_1 = m'$
- Upon receiving the challenge ciphertext $\bar{c}$
  - If $\bar{c} \in \mathcal{C}_{m'}$, output a random guess $b' \in \{0, 1\}$
  - Otherwise output $b' = 0$

Running time?

Can be exponential: we need to check all keys to decide if $\bar{c} \in C_{m'}$

Advantage?

Another concrete attack: advantage?

If $b = 1$, then $m_1 = m'$ was encrypted and $\bar{c} \in \mathcal{C}_{m'}$

Another concrete attack: advantage?

If $b = 1$, then $m_1 = m'$ was encrypted and $\bar{c} \in \mathcal{C}_{m'}$ $\quad \Longrightarrow$ b' is chosen uniformly at random

Another concrete attack: advantage?

If $b = 1$, then $m_1 = m'$ was encrypted and $\bar{c} \in \mathcal{C}_{m'}$ $\quad \Longrightarrow$ b' is chosen uniformly at random

$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$

Another concrete attack: advantage?

If $b = 1$, then $m_1 = m'$ was encrypted and $\bar{c} \in \mathcal{C}_{m'}$ $\implies$ b' is chosen uniformly at random

$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$

If $b = 0$, then $m_0 = m$ was encrypted:

Another concrete attack: advantage?

If $b = 1$, then $m_1 = m'$ was encrypted and $\bar{c} \in \mathcal{C}_{m'}$ $\implies$ b' is chosen uniformly at random

$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$

If $b = 0$, then $m_0 = m$ was encrypted:

- With probability $1 - \varepsilon$, $\bar{c} \in \mathcal{C}_{m'}$ and b' is chosen uniformly at random

Another concrete attack: advantage?

If $b = 1$, then $m_1 = m'$ was encrypted and $\bar{c} \in \mathcal{C}_{m'}$ $\implies$ b' is chosen uniformly at random

$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$

If $b = 0$, then $m_0 = m$ was encrypted:

- With probability $1 - \varepsilon$, $\bar{c} \in \mathcal{C}_{m'}$ and b' is chosen uniformly at random
- With probability ε, $c \notin \mathcal{C}_{m'}$ and $b' = 0$

Another concrete attack: advantage?

If $b = 1$, then $m_1 = m'$ was encrypted and $\bar{c} \in \mathcal{C}_{m'}$ $\quad \implies$ b' is chosen uniformly at random

$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$

If $b = 0$, then $m_0 = m$ was encrypted:

- With probability $1 - \varepsilon$, $\bar{c} \in \mathcal{C}_{m'}$ and b' is chosen uniformly at random
- With probability ε, $c \notin \mathcal{C}_{m'}$ and $b' = 0$

$\Pr[b' = 0 \mid b = 0] = (1 - \varepsilon) \cdot \frac{1}{2} + \varepsilon \cdot 1 = \frac{1}{2} + \frac{\varepsilon}{2}$

Another concrete attack: advantage?

If $b = 1$, then $m_1 = m'$ was encrypted and $\bar{c} \in \mathcal{C}_{m'}$ $\implies$ b' is chosen uniformly at random

$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$

If $b = 0$, then $m_0 = m$ was encrypted:

- With probability $1 - \varepsilon$, $\bar{c} \in \mathcal{C}_{m'}$ and b' is chosen uniformly at random
- With probability ε, $c \notin \mathcal{C}_{m'}$ and $b' = 0$

$\Pr[b' = 0 \mid b = 0] = (1 - \varepsilon) \cdot \frac{1}{2} + \varepsilon \cdot 1 = \frac{1}{2} + \frac{\varepsilon}{2}$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \ = \Pr[b' = 0 \mid b = 0] \Pr[b = 0] + \Pr[b' = 1 \mid b = 1] \Pr[b = 1]$

Another concrete attack: advantage?

If $b = 1$, then $m_1 = m'$ was encrypted and $\bar{c} \in \mathcal{C}_{m'}$ $\quad \implies$ b' is chosen uniformly at random

$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$

If $b = 0$, then $m_0 = m$ was encrypted:

- With probability $1 - \varepsilon$, $\bar{c} \in \mathcal{C}_{m'}$ and b' is chosen uniformly at random
- With probability ε, $c \notin \mathcal{C}_{m'}$ and $b' = 0$

$\Pr[b' = 0 \mid b = 0] = (1 - \varepsilon) \cdot \frac{1}{2} + \varepsilon \cdot 1 = \frac{1}{2} + \frac{\varepsilon}{2}$

$$\begin{aligned}\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] &= \Pr[b' = 0 \mid b = 0] \Pr[b = 0] + \Pr[b' = 1 \mid b = 1] \Pr[b = 1] \\ &= (\tfrac{1}{2} + \tfrac{\epsilon}{2}) \cdot \tfrac{1}{2} + \tfrac{1}{2} \cdot \tfrac{1}{2}\end{aligned}$$

Another concrete attack: advantage?

If $b = 1$, then $m_1 = m'$ was encrypted and $\bar{c} \in \mathcal{C}_{m'}$ $\implies$ b' is chosen uniformly at random

$\Pr[b' = 1 \mid b = 1] = \frac{1}{2}$

If $b = 0$, then $m_0 = m$ was encrypted:

- With probability $1 - \varepsilon$, $\bar{c} \in \mathcal{C}_{m'}$ and b' is chosen uniformly at random
- With probability ε, $c \notin \mathcal{C}_{m'}$ and $b' = 0$

$\Pr[b' = 0 \mid b = 0] = (1 - \varepsilon) \cdot \frac{1}{2} + \varepsilon \cdot 1 = \frac{1}{2} + \frac{\varepsilon}{2}$

$$\begin{aligned} \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] &= \Pr[b' = 0 \mid b = 0] \Pr[b = 0] + \Pr[b' = 1 \mid b = 1] \Pr[b = 1] \\ &= (\tfrac{1}{2} + \tfrac{\epsilon}{2}) \cdot \tfrac{1}{2} + \tfrac{1}{2} \cdot \tfrac{1}{2} \quad = \tfrac{1}{2} + \tfrac{\varepsilon}{4} \end{aligned}$$

Advantage!

Another concrete attack: advantage?

$\Pr[\mathsf{Enc}_K(m) \in \mathcal{C}_{m'}] = 1 - \varepsilon$ for some $\varepsilon > 0$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} + \frac{\varepsilon}{4}$

How big is ε?

Another concrete attack: advantage?

$\Pr[\mathsf{Enc}_K(m) \in \mathcal{C}_{m'}] = 1 - \varepsilon$ for some $\varepsilon > 0$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} + \frac{\varepsilon}{4}$

How big is ε?

If keys are just one bit shorter than the messages then there is a pair of messages m, m' for which $\varepsilon \geq \frac{1}{2}$

See, e.g., Theorem 17.9 in “A Course in Cryptography” (3rd edition) by Rafael Pass and Abhi Shelat for a proof.

Another concrete attack: advantage?

$\Pr[\mathsf{Enc}_K(m) \in \mathcal{C}_{m'}] = 1 - \varepsilon$ for some $\varepsilon > 0$

$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2} + \frac{\varepsilon}{4} \quad \geq 62.5\%$

How big is ε?

If keys are just one bit shorter than the messages then there is a pair of messages m, m' for which $\varepsilon \geq \frac{1}{2}$

The advantage is is at least $\frac{1}{8}$!

See, e.g., Theorem 17.9 in “A Course in Cryptography” (3rd edition) by Rafael Pass and Abhi Shelat for a proof.

Limitations of Perfect Secrecy

In Alice's version of OTP we have $|\mathcal{K}| < |\mathcal{M}|$, therefore the scheme cannot be perfectly secure!

Limitations of Perfect Secrecy

In Alice's version of OTP we have $|\mathcal{K}| < |\mathcal{M}|$, therefore the scheme cannot be perfectly secure!

No private-key encryption scheme can handle arbitrarily long messages and be perfectly secret (recall that $\mathcal{K}$ is a finite set).

Limitations of Perfect Secrecy

In Alice's version of OTP we have $|\mathcal{K}| < |\mathcal{M}|$, therefore the scheme cannot be perfectly secure!

No private-key encryption scheme can handle arbitrarily long messages and be perfectly secret (recall that $\mathcal{K}$ is a finite set).

Individuals occasionally claim they have developed a radically new encryption scheme that is "unbreakable" and achieves the security of the one-time pad without using keys as long as what is being encrypted. [...] Anyone making such claims either knows very little about cryptography or is blatantly lying.

Shannon's Theorem

Shannon's Theorem: *Let* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $\mathit{Enc}_k(m) = c$*.*

Proof:

Shannon's Theorem

Shannon's Theorem: *Let* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. *The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$, *there is a unique key* $k \in \mathcal{K}$ *such that* $\mathit{Enc}_k(m) = c$.

Proof:

1 & 2 $\implies$ perfect secrecy.

Pick any pair of messages $m, m' \in \mathcal{M}$ and any $c \in \mathcal{C}$.

Shannon's Theorem

Shannon's Theorem: *Let* (Gen, Enc, Dec) *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $\textit{Enc}_k(m) = c$*.*

Proof:

1 & 2 $\implies$ perfect secrecy.

Pick any pair of messages $m, m' \in \mathcal{M}$ and any $c \in \mathcal{C}$.

Let k (resp. k') the unique key such that $\text{Enc}_k(m) = c$ (resp. $\text{Enc}_{k'}(m') = c$).

Shannon's Theorem

Shannon's Theorem: *Let* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $\mathsf{Enc}_k(m) = c$*.*

Proof:

1 & 2 $\implies$ perfect secrecy.

Pick any pair of messages $m, m' \in \mathcal{M}$ and any $c \in \mathcal{C}$.

Let k (resp. k') the unique key such that $\mathsf{Enc}_k(m) = c$ (resp. $\mathsf{Enc}_{k'}(m') = c$).

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[K = k] = \frac{1}{|\mathcal{K}|}$$

Shannon's Theorem

Shannon's Theorem: *Let* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $\mathit{Enc}_k(m) = c$*.*

Proof:

1 & 2 $\implies$ perfect secrecy.

Pick any pair of messages $m, m' \in \mathcal{M}$ and any $c \in \mathcal{C}$.

Let k (resp. k') the unique key such that $\mathsf{Enc}_k(m) = c$ (resp. $\mathsf{Enc}_{k'}(m') = c$).

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[K = k] = \frac{1}{|\mathcal{K}|} = \Pr[K = k'] = \Pr[\mathsf{Enc}_K(m') = c]$$

Shannon's Theorem

Shannon's Theorem: *Let* (Gen, Enc, Dec) *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $\mathit{Enc}_k(m) = c$*.*

Proof:

perfect secrecy $\implies$ 2.

Fix any $m^* \in \mathcal{M}, c \in \mathcal{C}$ such that $\Pr[\mathsf{Enc}_K(m^*) = c] \neq 0$

Shannon's Theorem

Shannon's Theorem: *Let* (Gen, Enc, Dec) *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. *The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $\mathit{Enc}_k(m) = c$.

Proof:

perfect secrecy $\implies$ 2.

Fix any $m^* \in \mathcal{M}, c \in \mathcal{C}$ such that $\Pr[\mathsf{Enc}_K(m^*) = c] \neq 0$

For each $m_i \in \mathcal{M}$ there must be at least one key k such that $\mathsf{Enc}_k(m_i) = c$
(since $\Pr[\mathsf{Enc}_K(m_i) = c] = \Pr[\mathsf{Enc}_K(m^*) = c] \neq 0$)

Shannon's Theorem

Shannon's Theorem: *Let* (Gen, Enc, Dec) *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*.*
The scheme is perfectly secret if and only if:

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $\mathsf{Enc}_k(m) = c$*.*

Proof:

perfect secrecy $\implies$ 2.

Fix any $m^* \in \mathcal{M}, c \in \mathcal{C}$ such that $\Pr[\mathsf{Enc}_K(m^*) = c] \neq 0$

For each $m_i \in \mathcal{M}$ there must be at least one key k such that $\mathsf{Enc}_k(m_i) = c$
(since $\Pr[\mathsf{Enc}_K(m_i) = c] = \Pr[\mathsf{Enc}_K(m^*) = c] \neq 0$)

Let K_i be the set of keys k such that $\mathsf{Enc}_k(m_i) = c$

Shannon's Theorem

Shannon's Theorem: *Let* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. *The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$, *there is a unique key* $k \in \mathcal{K}$ *such that* $\mathit{Enc}_k(m) = c$.

Proof:

perfect secrecy $\implies$ 2.

Fix any $m^* \in \mathcal{M}, c \in \mathcal{C}$ such that $\Pr[\mathsf{Enc}_K(m^*) = c] \neq 0$

For each $m_i \in \mathcal{M}$ there must be at least one key k such that $\mathsf{Enc}_k(m_i) = c$
(since $\Pr[\mathsf{Enc}_K(m_i) = c] = \Pr[\mathsf{Enc}_K(m^*) = c] \neq 0$)

Let K_i be the set of keys k such that $\mathsf{Enc}_k(m_i) = c$

- For all m_i, $|K_i| \geq 1$
- Each key k belongs to at most one set K_i (otherwise two plaintexts encrypt to the same ciphertexts with the same key)

Shannon's Theorem

Shannon's Theorem: *Let $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ be an encryption scheme with $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. The scheme is perfectly secret if and only if:*

1. *Every key in $\mathcal{K}$ is chosen with probability $\frac{1}{|\mathcal{K}|}$ by Gen.*
2. *For every $m \in \mathcal{M}$ and every $c \in \mathcal{C}$, there is a unique key $k \in \mathcal{K}$ such that $\mathit{Enc}_k(m) = c$.*

Proof:

perfect secrecy $\implies$ 2.

Fix any $m^* \in \mathcal{M}, c \in \mathcal{C}$ such that $\Pr[\mathsf{Enc}_K(m^*) = c] \neq 0$

For each $m_i \in \mathcal{M}$ there must be at least one key k such that $\mathsf{Enc}_k(m_i) = c$
(since $\Pr[\mathsf{Enc}_K(m_i) = c] = \Pr[\mathsf{Enc}_K(m^*) = c] \neq 0$)

Let K_i be the set of keys k such that $\mathsf{Enc}_k(m_i) = c$

- For all m_i, $|K_i| \geq 1$
- Each key k belongs to at most one set K_i (otherwise two plaintexts encrypt to the same ciphertexts with the same key)

$\left.\right\} \implies$ For all m_i, $|K_i| = 1$

Shannon's Theorem

Shannon's Theorem: *Let* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $\mathit{Enc}_k(m) = c$*.*

Proof:

perfect secrecy $\implies$ 1.

For each key $k_i \in \mathcal{K}$ (resp. k_j), there is a unique set K_i (resp. K_j) containing k_i (resp. k_j).

Shannon's Theorem

Shannon's Theorem: *Let* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $\mathit{Enc}_k(m) = c$*.*

Proof:

perfect secrecy $\implies$ 1.

For each key $k_i \in \mathcal{K}$ (resp. k_j), there is a unique set K_i (resp. K_j) containing k_i (resp. k_j).

$$\Pr[K = k_i] = \Pr[\mathsf{Enc}_K(m_i) = c] = \Pr[\mathsf{Enc}_K(m_j) = c] = \Pr[K = k_j]$$

$\square$

Proof of security of One-Time pad, revisited

Shannon's Theorem: *Let* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. *The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$, *there is a unique key* $k \in \mathcal{K}$ *such that* $\mathit{Enc}_k(m) = c$.

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof:

Proof of security of One-Time pad, revisited

Shannon's Theorem: *Let* (Gen, Enc, Dec) *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. *The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$, *there is a unique key* $k \in \mathcal{K}$ *such that* $Enc_k(m) = c$.

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof:

- $\mathcal{M} = \mathcal{K} = \mathcal{C}$ therefore $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$

Proof of security of One-Time pad, revisited

Shannon's Theorem: *Let* (Gen, Enc, Dec) *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $Enc_k(m) = c$*.*

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof:

- $\mathcal{M} = \mathcal{K} = \mathcal{C}$ therefore $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$
- Every key is chosen with probability $\frac{1}{2^\ell} = \frac{1}{|\mathcal{K}|}$

Proof of security of One-Time pad, revisited

Shannon's Theorem: *Let* (Gen, Enc, Dec) *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. *The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $Enc_k(m) = c$.

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof:

- $\mathcal{M} = \mathcal{K} = \mathcal{C}$ therefore $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$
- Every key is chosen with probability $\frac{1}{2^\ell} = \frac{1}{|\mathcal{K}|}$
- Given m and c, there is a unique key k such that $\text{Enc}_k(m) = c$, namely $c \oplus m$ (recall that $\text{Enc}_k(m) = k \oplus m$)

Proof of security of One-Time pad, revisited

Shannon's Theorem: *Let* $(\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ *be an encryption scheme with* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. The scheme is perfectly secret if and only if:*

1. *Every key in* $\mathcal{K}$ *is chosen with probability* $\frac{1}{|\mathcal{K}|}$ *by Gen.*
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there is a unique key* $k \in \mathcal{K}$ *such that* $\mathit{Enc}_k(m) = c$*.*

Theorem: The one-time pad encryption scheme is perfectly secret.

Proof:

- $\mathcal{M} = \mathcal{K} = \mathcal{C}$ therefore $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$
- Every key is chosen with probability $\frac{1}{2^\ell} = \frac{1}{|\mathcal{K}|}$
- Given m and c, there is a unique key k such that $\mathsf{Enc}_k(m) = c$, namely $c \oplus m$ (recall that $\mathsf{Enc}_k(m) = k \oplus m$)

The claim follows from Shannon's theorem. $\square$