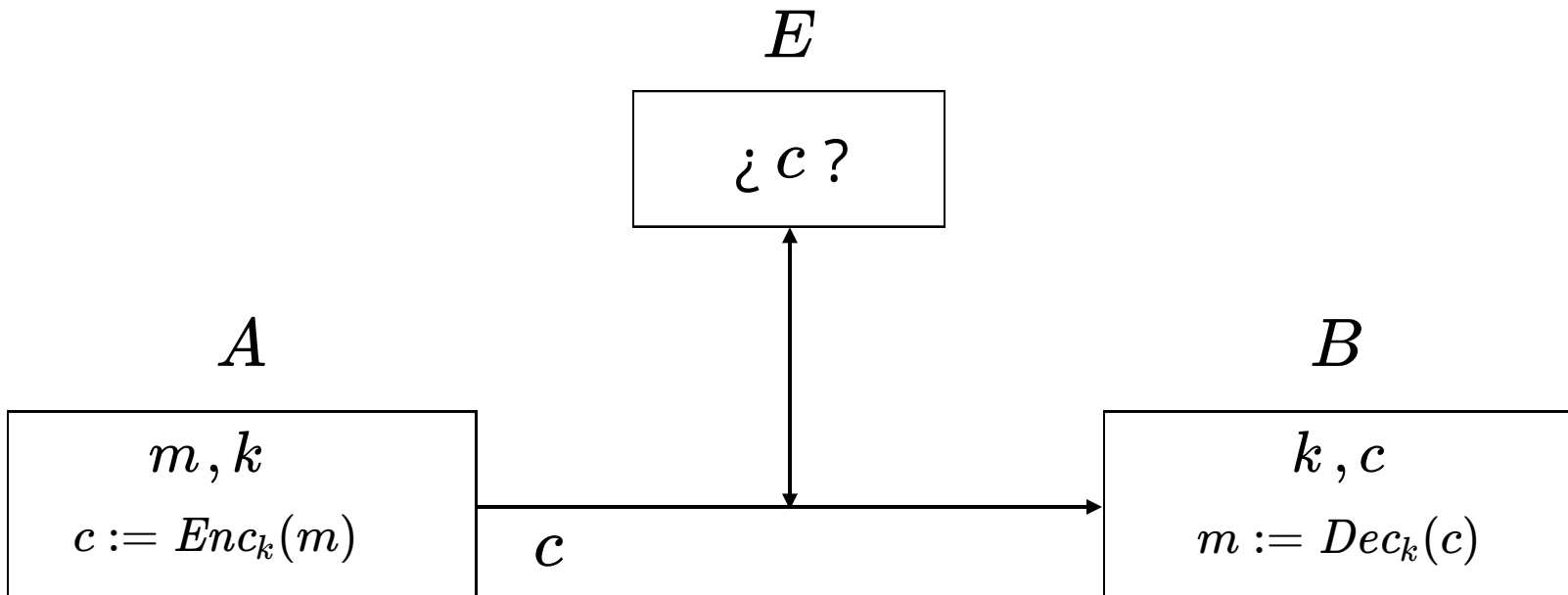


# IIC3253

OTP y perfect secrecy

# Cifrado (simétrico)



# Cifrado del César

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

HOLA MUNDO  
EMIX JRKAM

MANDEN BITCOINS A UCRANIA  
JXKABK YFQZMFKP X RZOXKFX

¿Problemas?

# Cifrado del César + llave

Llave = shift

7

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

HOLA MUNDO

AIET FÑGWI

MANDEN BITCOINS A UCRANIA

FTGWXG UBNVIBGM T ÑVLTGBT

¿Problemas?

La probabilidad de que un atacante "seleccione" o "adivine" la llave correcta debe ser muy baja.

⇒ El espacio de llaves posibles debe ser muy (muy) grande

¿Cómo podríamos agrandar el espacio de llaves siguiendo la idea de "sustituir"?

# Shift → Permutación

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

HOLA MUNDO

RHKP AZJWH

¿Cuántas llaves posibles?

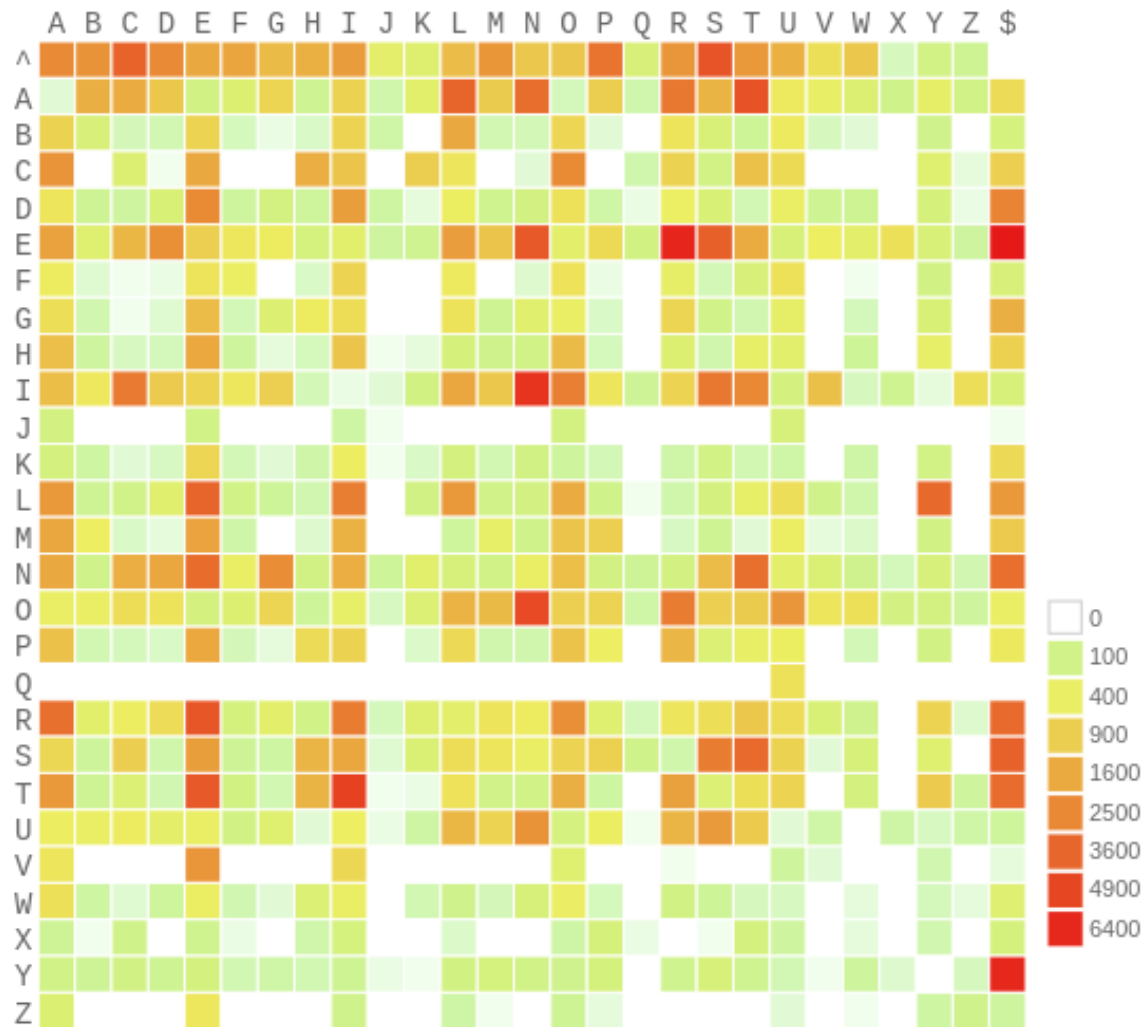
$27! = 10,888,869,450,418,352,160,768,000,000$

# ¿Es este un buen cifrado?

## | The Most Used Letters in English

WordCheats.com







Un espacio de  
llaves grande  
es necesario,  
no suficiente.

**ONE-TIME PAD (OTP)**

# Operación Módulo

(Recordatorio)

Dados  $a, n \in \mathbb{Z}$ , existe un único par de elementos  $(q, r) \in \mathbb{Z}^2$  tal que:

$$0 \leq r < |n|$$

$$a = q \cdot n + r$$

  
Cuociente                      Resto

Decimos entonces que  $a \bmod n = r$  y que  $a \equiv r \bmod n$

# Operación Módulo

(Ejemplos)

$$10 \bmod 3 = 1$$

$$28 \bmod 8 = 4$$

$$6 \bmod -20 = 6$$

$$-6 \bmod -20 = 14$$

Siempre esperaríamos que

$$n \cdot \left\lfloor \frac{a}{n} \right\rfloor + (a \bmod n) = a$$

Programando, esto se ve como

$$\mathbf{n} * (\mathbf{a} / \mathbf{n}) + \mathbf{a} \% \mathbf{n} = \mathbf{a}$$

División entera



```
1 # Python
2 print("La división entera entre 6 y -20 es:")
3 print(6 // -20)
```

Output: -1

```
1 // C++
2 #include <iostream>
3 using namespace std;
4
5 int main() {
6     cout << "La división entera entre 6 y -20 es: " << endl;
7     cout << (6 / 20) << endl;
8     return 0;
9 }
```

Output: 0



Esperamos que

$$n * (a / n) + a \% n = a$$

$$-20 * (6 / -20) + 6 \% -20 = 6$$

Python:  $-20 * -1 + 6 \% -20 = 6 \quad \Rightarrow 6 \% -20 = -14$

C++:  $-20 * 0 + 6 \% -20 = 6 \quad \Rightarrow 6 \% -20 = 6$



# Operación Módulo

Dados  $a, n \in \mathbb{Z}$ , existe un único par de elementos  $(q, r) \in \mathbb{Z}^2$  tal que:

$$0 \leq r < |n|$$

$$a = q \cdot n + r$$

Decimos entonces que  $a \bmod n = r$  y que  $a \equiv r \bmod n$



# ONE-TIME PAD (OTP)

# Partimos enumerando las letras

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Para enviar un mensaje de largo  $\ell$   
necesitaremos una llave de largo  $\ell$

Diagram illustrating the Vigenere cipher encryption process:

HOLAMUNDO	→	7	15	11	0	12	21	13	3	15
SECRETKEY	+	19	4	2	18	4	20	10	4	25
		<hr/>								
mod 27		26	19	13	18	16	41	23	7	40
		<hr/>								
ZSNRPÑWHN	←	26	19	13	18	16	14	23	7	13
↓										
texto cifrado										

$$Enc_{SECRETKEY}(HOLAMUNDO) = ZSNRP\tilde{N}WHN$$

¿Cómo decriptar?

$$Dec_{SECRETKEY}(ZSNRP\tilde{N}WHN) = HOLAMUNDO$$

ZSNRP $\tilde{N}$ WHN	➡	26 19 13 18 16 14 23 7 13
SECRETKEY		— 19 4 2 18 4 20 10 4 25
		mod 27 7 15 11 0 12 -6 13 3 -12
HOLAMUNDO	⬅	7 15 11 0 12 21 13 3 15

A	B	C	D	E	F	G	H	I	J	K	L	M	N	$\tilde{N}$	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26



**La semana pasada...**

El operador módulo en lenguajes de programación...

$$n * (a / n) + a \% n = a$$

División entera

Si  $7 / -15 = -1$  entonces  $7 \% -15 = -8$

Si  $7 / -15 = 0$  entonces  $7 \% -15 = 7$

Si nos mantenemos **siempre** en módulo  
-15 entonces todo funciona bien.

¿Si salimos de ese mundo?

$$56 \div (7 \% -15) + 8 = \begin{matrix} 1 \\ 16 \end{matrix}$$

Al menos  $1 \equiv 16 \pmod{-15}$

¿Si aplicamos otros módulos?

$$10 \% (7 \% -15) = \begin{matrix} -6 \\ 3 \end{matrix}$$

Aquí tenemos:

$$3 \not\equiv -6 \pmod{-15} \quad 3 \not\equiv -6 \pmod{7} \quad 3 \not\equiv -6 \pmod{-8}$$

# ONE-TIME PAD (OTP)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Para enviar un mensaje de largo  $\ell$   
necesitaremos una llave de largo  $\ell$

HOLAMUNDO	→	7	15	11	0	12	21	13	3	15
SECRETKEY	+	19	4	2	18	4	20	10	4	25
		<hr/>								
	mod 27	26	19	13	18	16	41	23	7	40
		<hr/>								
ZSNRPÑWHN	←	26	19	13	18	16	14	23	7	13
↓										
texto cifrado										

## ¿Cómo decriptar?

ZSNRPÑWHN  
SECRETKEY



$$\begin{array}{r} 26 \ 19 \ 13 \ 18 \ 16 \ 14 \ 23 \ 7 \ 13 \\ - 19 \ 4 \ 2 \ 18 \ 4 \ 20 \ 10 \ 4 \ 25 \\ \hline \text{mod } 27 \ 7 \ 15 \ 11 \ 0 \ 12 \ -6 \ 13 \ 3 \ -12 \\ \hline \end{array}$$

HOLAMUNDO



7 15 11 0 12 21 13 3 15





## ¿Cómo decriptar?

$$\begin{array}{rcl} \text{ZSNRPÑWHN} & \xrightarrow{\quad} & \begin{array}{cccccccccc} 26 & 19 & 13 & 18 & 16 & 14 & 23 & 7 & 13 \\ 19 & 4 & 2 & 18 & 4 & 20 & 10 & 4 & 25 \end{array} \\ \text{SECRETKEY} & & \hline & \text{mod } 27 & \begin{array}{cccccccccc} 7 & 15 & 11 & 0 & 12 & -6 & 13 & 3 & -12 \end{array} \\ & & \hline \text{HOLAMUNDO} & \xleftarrow{\quad} & \begin{array}{cccccccccc} 7 & 15 & 11 & 0 & 12 & 21 & 13 & 3 & 15 \end{array} \end{array}$$

Para formalizarlo necesitamos convertir mensajes, llaves y textos cifrados en arreglos de enteros

$$m = \text{HOLAMUNDO}$$

$$\bar{m} = (7, 15, 11, 0, 12, 21, 13, 3, 15)$$

$$k = \text{SECRETKEY}$$

$$\bar{k} = (19, 4, 2, 18, 4, 20, 10, 4, 25)$$

$$c = \text{ZSNRPÑWHN}$$

$$\bar{c} = (26, 19, 13, 18, 16, 14, 23, 7, 13)$$

De la misma forma necesitamos hacer  
la conversión en la otra dirección

$$a = (4, 9, 4, 12, 16, 11, 15) \quad \bar{a} = \text{EJEMPLO}$$

Naturalmente, siempre se cumple que  $\overline{\bar{s}} = s$

Con esto definimos OTP en base a

$$Enc_k(m) = \overline{(\bar{m} + \bar{k}) \bmod 27}$$

$$Dec_k(c) = \overline{(\bar{c} - \bar{k}) \bmod 27}$$

Desde ahora supondremos que nuestros mensajes y llaves **son** arreglos de números

Definiremos OTP simplemente usando

$$Enc_k(m) = (m + k) \bmod 27$$

$$Dec_k(c) = (c - k) \bmod 27$$

$$Dec_k(Enc_k(m)) = ((m + k) \bmod 27 - k) \bmod 27$$

$$= (m + k - k) \bmod 27 = m \bmod 27 = m$$

Esperamos que para un esquema criptográfico  $(Gen, Enc, Dec)$  se cumpla

$$\forall k \in \mathcal{K} \forall m \in \mathcal{M} : Dec_k(Enc_k(m)) = m$$

En este caso diremos que el esquema es *perfectamente correcto*

¿Por qué *perfectamente*?

OTP: sobre  $\{0, 1, \dots, N - 1\}$  y mensajes de largo  $\ell$  ( $\text{OTP}^{N, \ell}$ )

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

*Gen* es la distribución uniforme sobre  $\{0, \dots, N - 1\}^\ell$

$$\text{Enc}_k(m) = (m + k) \bmod N$$

$$\text{Dec}_k(c) = (c - k) \bmod N$$

# ¿Qué tan bueno es OTP?

¿Qué pasa si veo un mensaje cifrado  $c$  pasar?

Aquí un ejemplo:

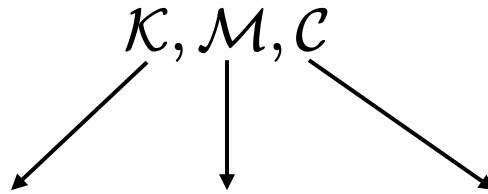
```
c = YFTGXEIWIWEHAGQGESLPKRVLMYGXSJIQZVIYHVBRJGNTR  
m = ESTEMENSAJEESLITERALMENTEIMPOSIBLEDEDESCRIPTAR  
k = UNACLAVEINADIVINABLEYNISISQUIERAPORFUERZABRUTA
```

# Perfect Secrecy



**La clase pasada...**

# Esquema criptográfico



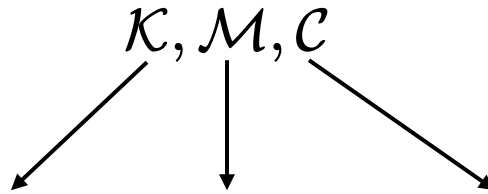
Espacio de llaves, mensajes y textos cifrados

Un esquema es un triple  $(Gen, Enc, Dec)$

$Gen$  es una distribución de probabilidades sobre  $\mathcal{K}$

Es decir,  $Gen : \mathcal{K} \rightarrow [0, 1]$  tal que  $\sum_{k \in \mathcal{K}} Gen(k) = 1$

# Esquema criptográfico



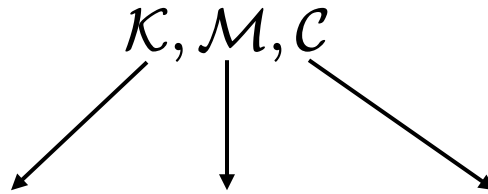
Espacio de llaves, mensajes y textos cifrados

Un esquema es un triple  $(Gen, Enc, Dec)$

$Enc = \{Enc_k \mid k \in \mathcal{K}\}$  es una familia de algoritmos para encriptar

Para cada  $k \in \mathcal{K}$ , se tiene que  $Enc_k : \mathcal{M} \rightarrow \mathcal{C}$

# Esquema criptográfico



Espacio de llaves, mensajes y textos cifrados

Un esquema es un triple  $(Gen, Enc, Dec)$

$Dec = \{Dec_k \mid k \in \mathcal{K}\}$  es una familia de algoritmos para  
decriptar

Para cada  $k \in \mathcal{K}$ , se tiene que  $Dec_k : \mathcal{C} \rightarrow \mathcal{M}$

¿Cuándo decimos que un esquema  
criptográfico es *perfectamente secreto*?

Pensemos en la idea de que si un atacante  
ve un texto cifrado *no gana información*.

Podríamos decir algo como lo siguiente:

*"Al ver un texto cifrado  $c_0$  pasar, para el atacante el mensaje original  $m$  podría haber sido cualquiera"*

¿Cómo formalizamos esto?

Dado un texto cifrado  $c_0$  se cumple que

$$\forall m_0 \in \mathcal{M} : \Pr_{k \sim \text{Gen}} [Enc_k(m_0) = c_0] = \frac{1}{|\mathcal{M}|}$$

$$\forall m_0 \in \mathcal{M} : \Pr_{k \sim \text{Gen}} [\text{Enc}_k(m_0) = c_0] = \frac{1}{|\mathcal{M}|}$$

¿Cómo se calcula esta probabilidad?

Es simplemente la probabilidad de haber elegido una llave que encripte  $m_0$  como  $c_0$

$$\sum_{k \in \mathcal{K} : \text{Enc}_k(m_0) = c_0} \text{Gen}(k)$$

¿Qué pasa si el atacante tenía información  
previa sobre el mensaje?

Por ejemplo sabe que el mensaje puede  
ser *"atacar ahora"* o *"emprender retirada"*

Podría incluso estimar que atacarán con probabilidad  $1/3$

¿Cómo modelamos esto matemáticamente?

Supondremos que el atacante tiene una  
distribución de probabilidad  $\mathbb{D}$  sobre  $\mathcal{M}$



Para cada distribución de probabilidad  $\mathbb{D}$  sobre  $\mathcal{M}$  y cada texto cifrado  $c_0 \in \mathcal{C}$  se cumple que

$$\forall m_0 \in \mathcal{M} : \Pr_{\substack{m \sim \mathbb{D} \\ k \sim \text{Gen}}} [m = m_0 \mid \text{Enc}_k(m) = c_0] = \Pr_{m \sim \mathbb{D}} [m = m_0]$$

Recordemos que  $\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}$

$$\frac{\mathbb{D}(m_0) \sum_{k \in \mathcal{K} : \text{Enc}_k(m_0) = c_0} \text{Gen}(k)}{\sum_{m \in \mathcal{M}} \mathbb{D}(m) \sum_{k \in \mathcal{K} : \text{Enc}_k(m) = c_0} \text{Gen}(k)} \stackrel{?}{=} \mathbb{D}(m_0)$$

¿Es  $\text{OTP}^{N,\ell}$  perfectamente secreto?

1.  $\text{Gen}$  es la distribución uniforme  $1/N^\ell$
2. Para cada  $c_0$  y cada  $m_0$  existe una única llave  $k$  tal que  $\text{Enc}_k(m_0) = c_0$

Sea  $c_0 \in \mathcal{C}$  un texto cifrado y  $m_0$  un mensaje.

$$\frac{\mathbb{D}(m_0) \sum_{k \in \mathcal{K} : \text{Enc}_k(m_0) = c_0} \text{Gen}(k)}{\sum_{m \in \mathcal{M}} \mathbb{D}(m) \sum_{k \in \mathcal{K} : \text{Enc}_k(m) = c_0} \text{Gen}(k)}$$

$$\frac{\mathbb{D}(m_0) \cdot \cancel{1/N^\ell}}{\sum_{m \in \mathcal{M}} \mathbb{D}(m) \cdot \cancel{1/N^\ell}} = \mathbb{D}(m_0)$$

1 ←

# ¿Definiciones alternativas?

1. La probabilidad de ver cualquier texto cifrado sin conocimiento previo es la misma que la probabilidad de ver dicho texto cifrado conociendo el mensaje de antemano.
2. La distribución de probabilidad sobre los mensajes es independiente de la distribución de probabilidad sobre los textos cifrados.

Ejercicio: formalizar estas nociones

**Un poco de historia**

# Julio César

# OTP



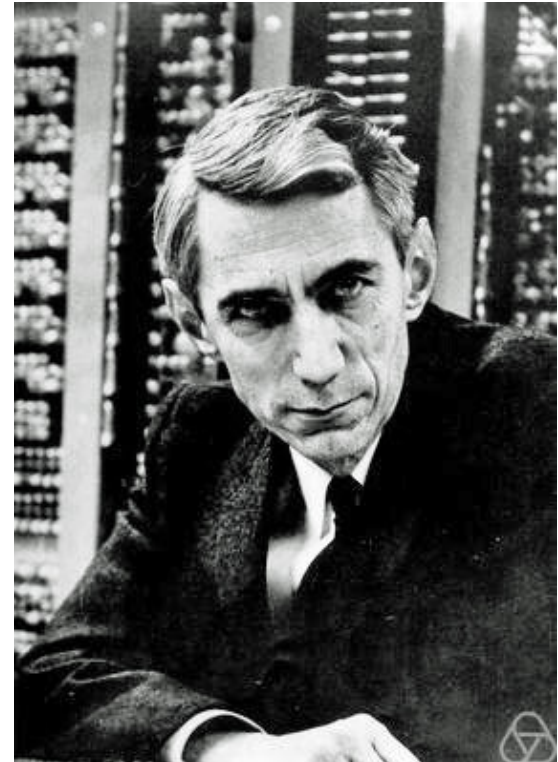
.....  
LFPHY ZANBR JXNKS JYMPF KQZAT  
VRETH JPCBU RVSTG JYANN ELBEL  
PQSTF JJJLVJ SPXNL NPLKA ZKVEY  
TQUDS XNNKJ NQSNB KPMPI QZVQZ  
ETJWV QNAKS PNTYV TTAKL ATQPN  
NHCJE PPNSV NQZLN QZTH CYQNS  
YIUVJ TRANE QNSES YQWU HQCKY  
HALPA NQINB SALSQ RQTN QZQNP  
QINPS QNPFQ ANBYJ CAYDS IQNNU  
QANEX QZJIN QNCEY QNHYE LPAAT  
● TI KPQPN INSEY QUVVE UITRN  
NQSNB QUNDS EPVJX QCEST PNTXK  
VEISE QNVTH QSNNS LQZNS UNVSK  
PPNPI QCPAA NLTKK QANDA QAINU  
NQINB QCTPF QVBNK QNNUK QCPKA  
ATQPS QNYSU QNYSX ITIPD QJCKK  
PPQPS QJQIN QYLLX QNTHC QNSHN  
PQNSA QYTLB QNKNR QANNA QNTHN  
QNSKA QJNPT QNUNH QNTHN QPLBY

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78
79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04
05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82
83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08
09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86
87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94
95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98
99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02
03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06
07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88
89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66
67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92
93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22
23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74
75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78
79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04
05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82
83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08
09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86
87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37</	

# Shannon (1945)

A Mathematical Theory  
of Cryptography

Primer desarrollo de  
fundamentos  
matemáticos de la  
criptografía





**Pero perfect secrecy  
es una condición  
muy fuerte**



# Lamentablemente...

Hemos discutido en clases que pareciera *molessto y/o poco razonable* que la llave tenga que ser tan larga como el mensaje.

¿Cómo modificamos OTP para tener  $|\mathcal{K}| < |\mathcal{M}|$  y seguir teniendo un esquema criptográfico *perfectamente secreto*?

No podemos 🤔

# Teorema

Sean  $\mathcal{M}, \mathcal{K}, \mathcal{C}$  espacios de mensajes, llaves y textos cifrados, respectivamente.

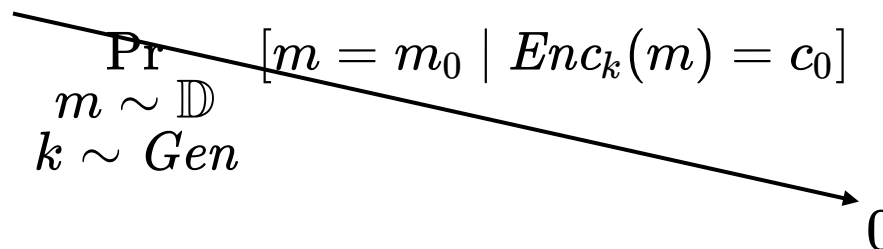
Si  $|\mathcal{K}| < |\mathcal{M}|$ , entonces no existe un esquema  $(Gen, Enc, Dec)$  que sea perfectamente secreto.

# Demostración

Supongamos que  $|\mathcal{K}| < |\mathcal{M}| \leq |\mathcal{C}|$  y sea  $(Gen, Enc, Dec)$  un esquema criptográfico

Sea  $\mathbb{D}$  una distribución sobre  $\mathcal{M}$  y  $m_0 \in \mathcal{M}$  un mensaje tal que  $\mathbb{D}(m_0) > 0$

Como  $|\mathcal{K}| < |\mathcal{M}| \leq |\mathcal{C}|$ , debe existir  $c_0 \in \mathcal{C}$  para el cual **ninguna** llave  $k \in \mathcal{K}$  satisface  $Enc_k(m_0) = c_0$

$$\Pr_{\substack{m \sim \mathbb{D} \\ k \sim Gen}} [m = m_0 \mid Enc_k(m) = c_0] < \mathbb{D}(m_0) = \Pr_{m \sim \mathbb{D}} [m = m_0]$$


Adiós perfect secrecy...



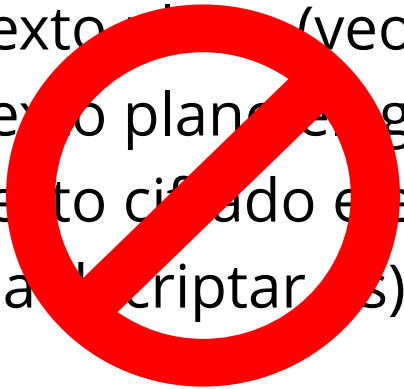
**Life is a series of closing doors, isn't it?**

# Back to reality

OTP y la noción de Perfect Secrecy son fundamentales para entender lo que viene

Pero en la práctica vamos a buscar otras propiedades...

¿Bajo qué modelo de ataque es OTP seguro?

1. Texto cifrado (sólo veo  $c_0, c_1, \dots$ )
  2. Texto cifrado y texto plano (veo  $(m_0, c_0), (m_1, c_1), \dots$ )
  3. Texto plano elegido (mando a encriptar  $m$ 's)
  4. Texto cifrado elegido (mando a encriptar  $m$ 's y a desencriptar  $c$ 's)
- 

## ¿Qué pasa si usamos llaves más cortas que el mensaje?

Pensemos por ejemplo en repetir la llave varias veces para encriptar un mensaje más largo que la llave

HOLAMUNDOCOMOTEHAIDO  
SECRETKEYSECRETKEYSE

 $+$ 

7 15 11 0 12 21 13 3 15 3 15 12 15 20 4 7 0 8 3 15  
19 4 2 18 4 20 10 4 25 19 4 2 18 4 20 10 4 25 19 4

 $\text{mod } 27$ 

26 19 13 18 16 41 23 7 40 22 19 14 33 24 24 17 4 33 22 19

ZSNRPÑWHNVSÑGXXQEGVS



26 19 13 18 16 14 23 7 13 22 19 14 6 24 24 17 4 6 22 19

texto cifrado

**¿Podemos quebrarlo?**