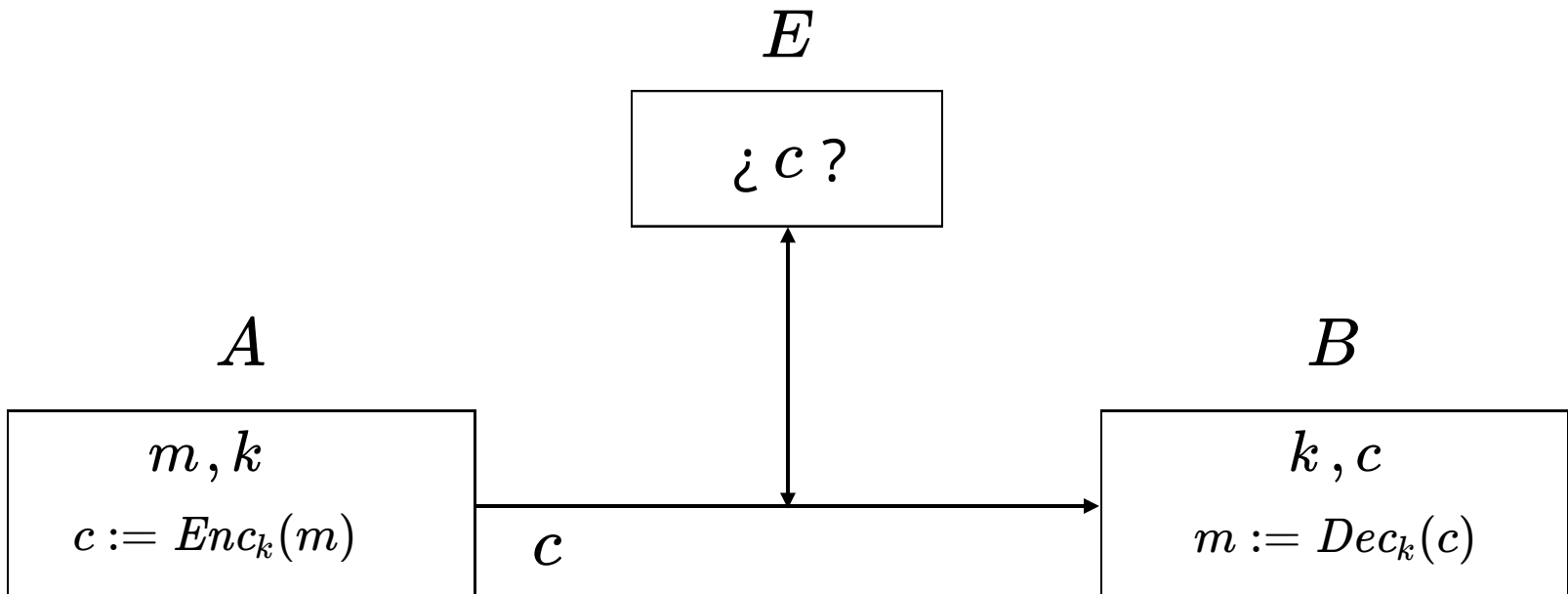


# IIC3253

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?

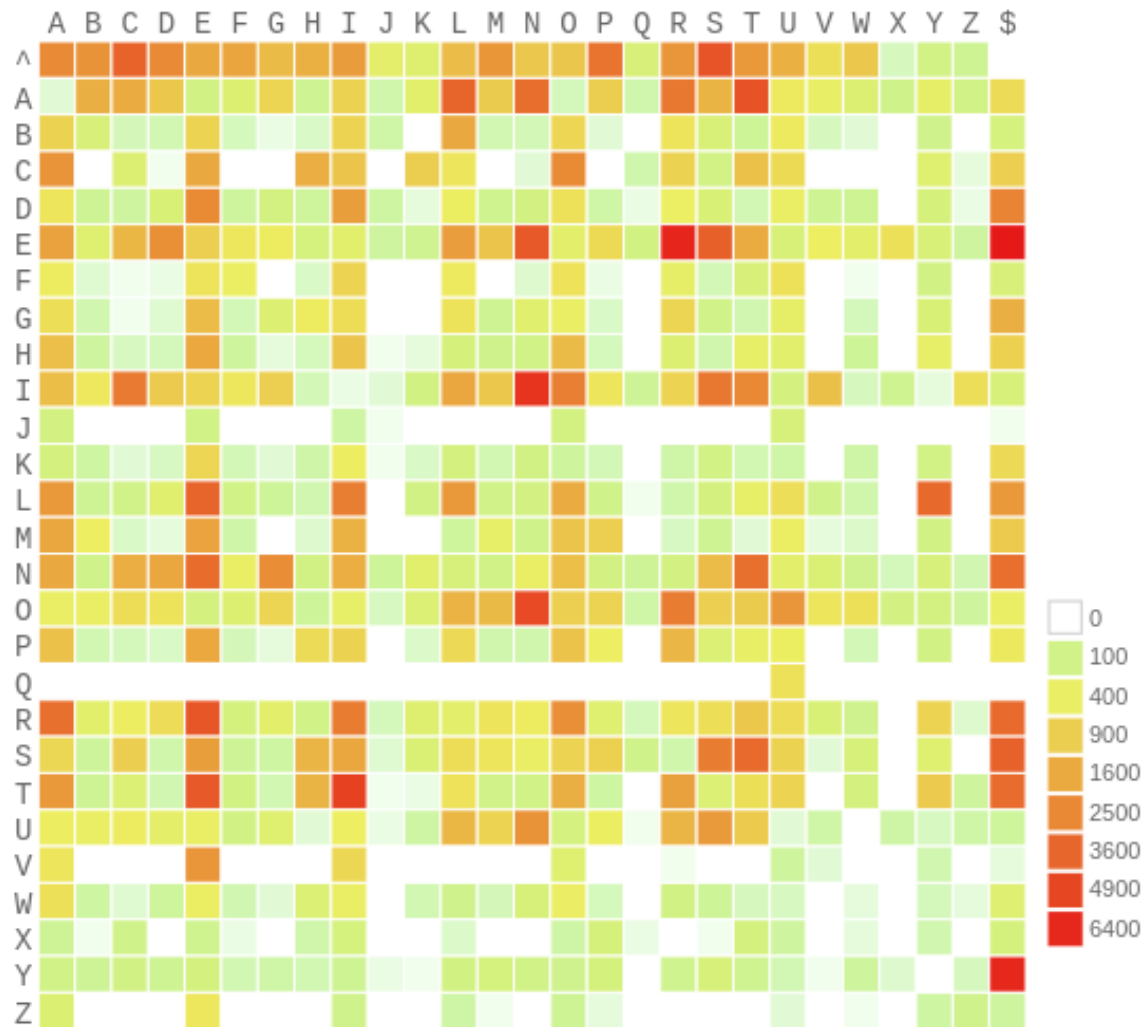
$27! = 10,888,869,450,418,352,160,768,000,000$

# ¿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  $a, n \in \mathbb{Z}$  con  $n \neq 0$ , 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  $a, n \in \mathbb{Z}$  con  $n \neq 0$ , 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 clase pasada...**

# Operación Módulo

Dados  $a, n \in \mathbb{Z}$  con  $n \neq 0$ , 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  $a \bmod n = r$

# Repaso de aritmética modular

Decimos que  $a \equiv b \pmod{n}$  si  $n$  divide a  $b - a$

- Por ejemplo:  $2 \equiv 7 \pmod{5}$ ,  $3 \equiv 23 \pmod{10}$   
y  $-2 \equiv 3 \pmod{5}$

Dos propiedades fundamentales:

- $a \equiv b \pmod{n}$  si y sólo si  $a \bmod n = b \bmod n$
- Si  $b = a \bmod n$ , entonces  $a \equiv b \pmod{n}$

# Repaso de aritmética modular

Otra propiedad fundamental: si  $a \equiv b \pmod{n}$   
y  $c \equiv d \pmod{n}$ , entonces:

$$(a + c) \equiv (b + d) \pmod{n}$$

$$(a \cdot c) \equiv (b \cdot d) \pmod{n}$$

# Repaso de aritmética modular

Una aplicación del resultado anterior:

$$(a + b) \bmod n = \\ (a \bmod n + b \bmod n) \bmod n$$



# 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/>								
			26	19	13	18	16	14	23	7	13
ZSNRPÑWHN	←										
↓											
texto cifrado											

## ¿Cómo decriptar?

ZSNRPÑWHN	→	26	19	13	18	16	14	23	7	13
SECRETKEY		19	4	2	18	4	20	10	4	25
		<hr/>								
	mod 27	7	15	11	0	12	-6	13	3	-12
		<hr/>								
HOLAMUNDO	←	7	15	11	0	12	21	13	3	15

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

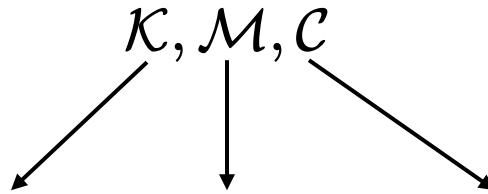
$$Enc_k(m) = (m + k) \bmod 27$$

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

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

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

# Esquema criptográfico



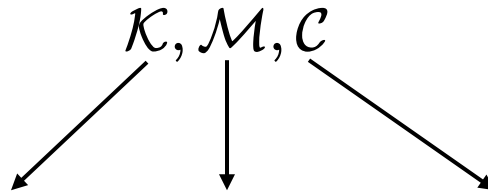
Espacio de llaves, mensajes y textos cifrados

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



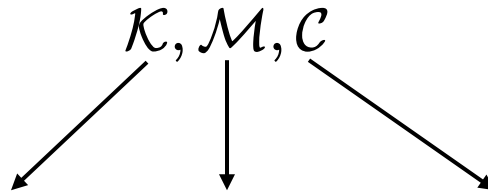
Espacio de llaves, mensajes y textos cifrados

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  $Dec_k : \mathcal{C} \rightarrow \mathcal{M}$

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

¿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



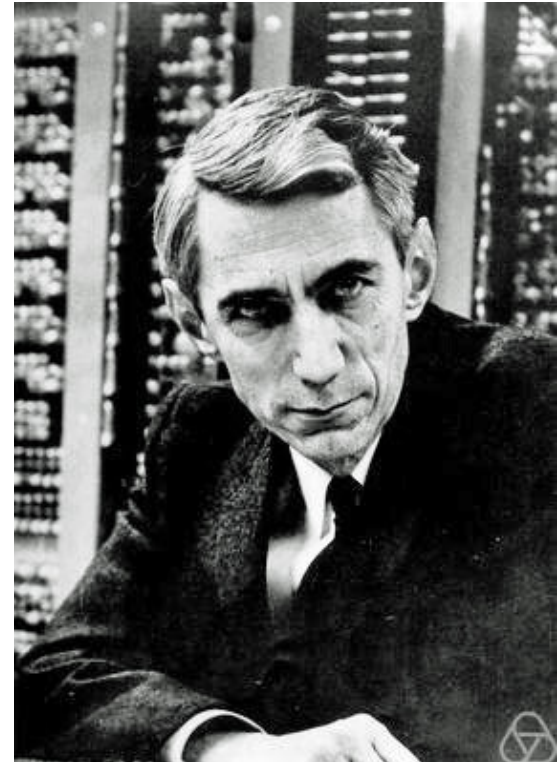
.....  
LFPHY ZANB JXKX STMP KZAT  
VRETH JPCBU RVSTB JXANN ELBEL  
PQSTV JLLVJ SPXNL NPLKA ZKVEY  
TQUBD XNNAJ NQSNB KPMPI QZVQZ  
ETJWV QNAKX PNTYV TTAKL ATQPN  
NHCJE PPABV BNZZN QZTH CYQNS  
VILUJ TRANK QNKEE YQWU HQCKY  
HALPA KXINB SAKDY KQTN ZQZNP  
QINPB QNPFQ KBBYJ CAYDS IQRNU  
QXKX QZJIN QNCEY KXVVC LPRAT  
● TI KPQPN INSEY KUVVC UITRN  
NQSNB ZUNDB EPVJX KCEYV PRTXK  
VEISE QVYTH QSNNA LQZNS UNVAK  
PPQPI KCPAA NLTKK DANDA BAINU  
KEINB LQTPP RVBNS KXVUK ACPKA  
ATQPS QNYSU QNYSX ITIPD KJCEK  
PPQPS JPAID NYLIX QNTHC QNSBN  
PQSPA QYTLB QNKAH KAPNA TQXBN  
QNSBA JXKPT HTUHN KQTN 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	100	101	102	103	104
105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156
157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182
183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208
209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234
235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260
261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286
287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312
313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338
339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364
365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390
391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416
417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442
443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468
469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494
495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520
521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546
547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572
573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598
599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624
625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650
651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676
677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702
703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728
729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754
755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780
781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806
807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832
833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858
859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884
885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910
911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936
937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962
963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988
989	990	991	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007	1008	1009	1010	1011	1012	1013	1014
1015	1016	1017	1018	1019	1020	1021	1022	1023	1024	1025	1026	1027	1028	1029	1030	1031	1032	1033	1034	1035	1036	1037	1038	1039	1040
1041	1042	1043	1044	1045	1046	1047	1048	1049	1050	1051	1052	1053	1054	1055	1056	1057	1058	1059	1060	1061	1062	1063	1064	1065	1066
1067	1068	1069	1070	1071	1072	1073	1074	1075	1076	1077	1078	1079	1080	1081	1082	1083	1084	1085	1086	1087	1088	1089	1090	1091	1092
1093	1094	1095	1096	1097	1098	1099	1100	1101	1102	1103	1104	1105	1106	1107	1108	1109	1110	1111	1112	1113	1114	1115	1116	1117	1118
1119	1120	1121	1122	1123	1124	1125	1126	1127	1128	1129	1130	1131	1132	1133	1134	1135	1136	1137	1138	1139	1140	1141	1142	1143	1144
1145	1146	1147	1148	1149	1150	1151	1152	1153	1154	1155	1156	1157	1158	1159	1160	1161	1162	1163	1164	1165	1166	1167	1168	1169	1170
1171	1172	1173	1174	1175	1176	1177	1178	1179	1180	1181	1182	1183	1184	1185	1186	1187	1188	1189	1190	1191	1192	1193	1194	1195	1196
1197	1198	1199	1200	1201	1202	1203	1204	1205	1206	1207	1208	1209	1210	1211	1212	1213	1214	1215	1216	1217	1218	1219	1220	1221	1222
1223	1224	1225	1226	1227	1228	1229	1230	1231	1232	1233	1234	1235	1236	1237	1238	1239	1240	1241	1242	1243	1244	1245	1246	1247	1248
1249	1250	1251	1252	1253	1254	1255	1256	1257	1258	1259	1260	1261	1262	1263	1264	1265	1266	1267	1268	1269	1270	1271	1272	1273	1274
1275	1276	1277	1278	1279	1280	1281	1282	1283	1284	1285	1286	1287	1288	1289	1290	1291	1292	1293	1294	1295	1296	1297	1298	1299	1300
1301	1302	1303	1304	1305	1306	1307	1308	1309	1310	1311	1312	1313	1314	1315	1316	1317	1318	1319	1320	1321	1322	1323	1324	1325	1326
1327	1328	1329	1330	1331	1332	1333	1334	1335	1336	1337	1338	1339	1340	1341	1342	1343	1344	1345	1346	1347	1348	1349	1350	1351	1352
1353	1354	1355	1356	1357	1358	1359	1360	1361	1362	1363	1364	1365	1366	1367	1368	1369	1370	1371	1372	1373	1374	1375	1376	1377	1378
1379	1380	1381	1382	1383	1384	1385	1386	1387	1388	1389	1390	1391	1392	1393	1394	1395	1396	1397	1398	1399	1400</				

# 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  $Enc_k(m_0) = c_0$

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

0

Adiós perfect secrecy...



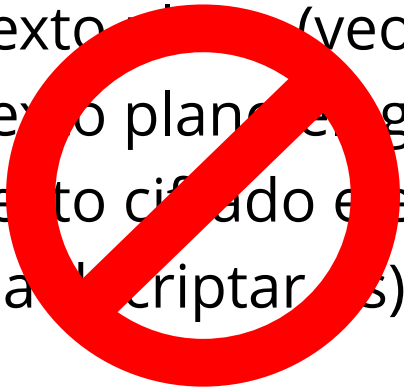
**Life is a series of closing doors, isn't it?**

# Back to reality

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

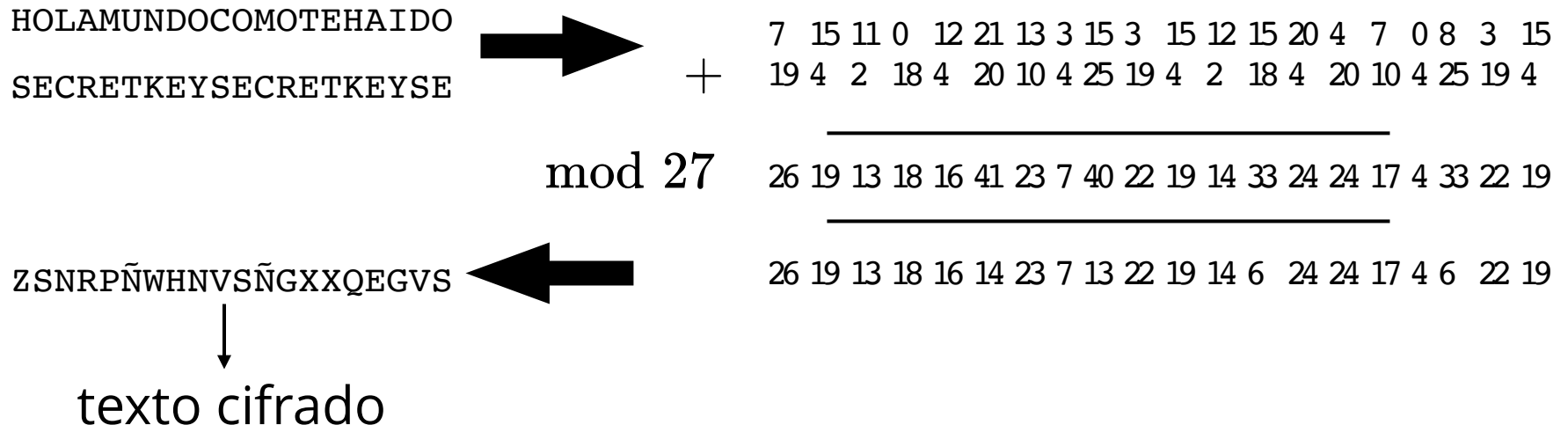
Pero en la práctica vamos a buscar otras propiedades...

¿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



**¿Podemos quebrarlo?**