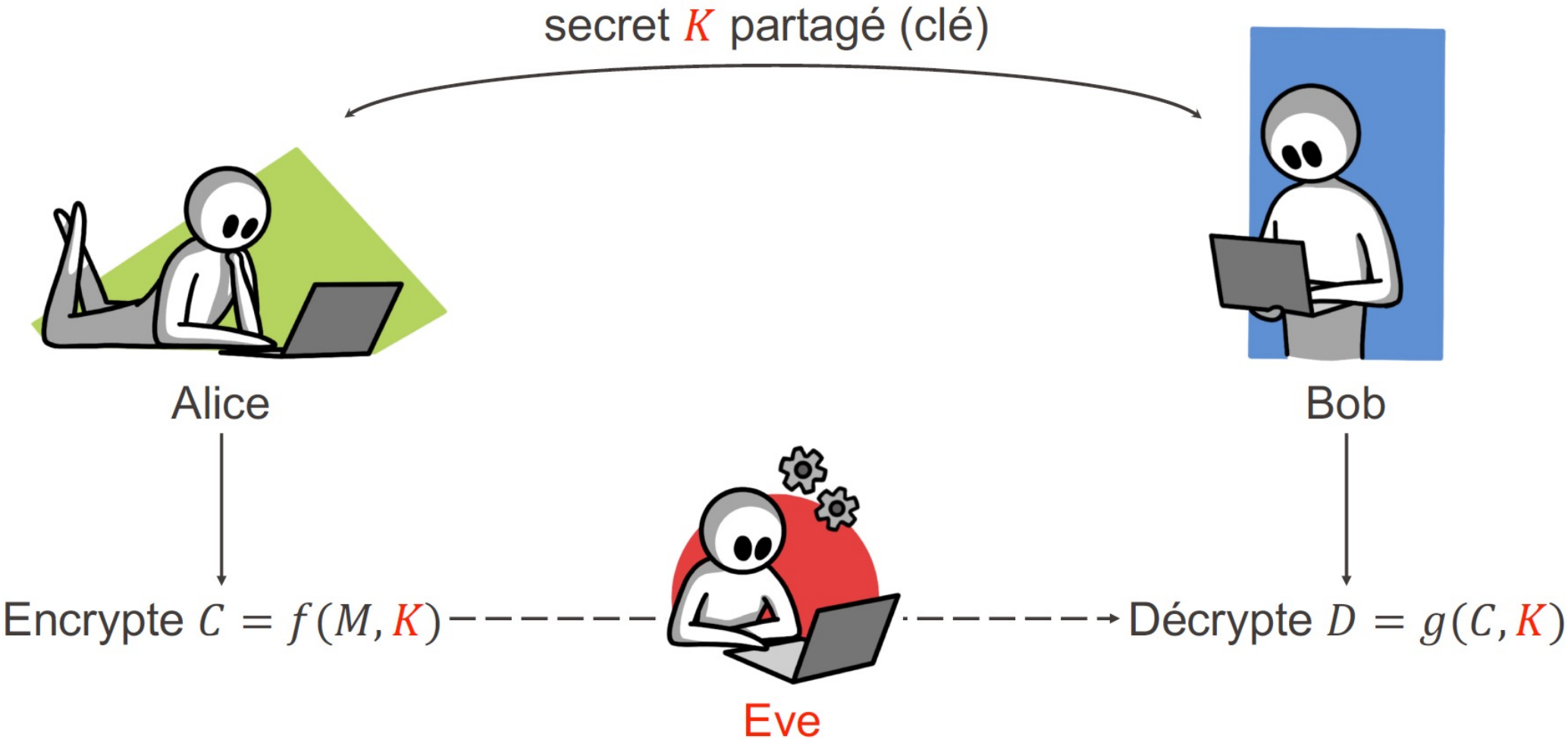
Cryptographie à clé secrète: suite

Cours Turing – Semaine 8

Rappel du scénario



Eve intercepte C mais ne sait pas trop quoi en faire sans la clé K…

Préliminaire: représentation binaire

Nombres entiers (positifs): $1984 = 1 \cdot 10^3 + 9 \cdot 10^2 + 8 \cdot 10^1 + 4 \cdot 10^0$

MCMLXXXIV

$1984 = 1024 + 512 + 256 + 128 + 64$

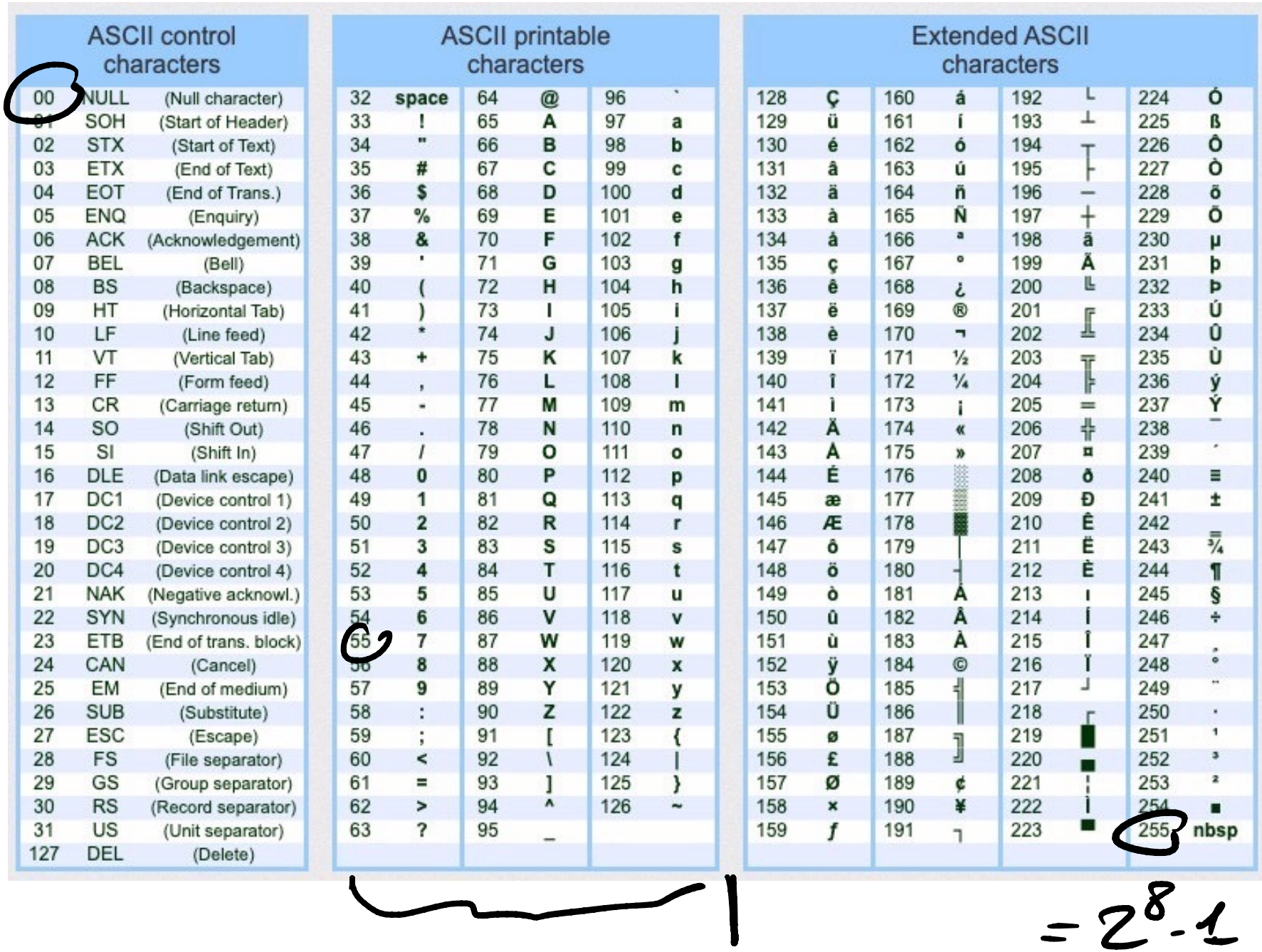
$= 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6$

$+ 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$

$= 11111000000$ en binaire

n bits $\longrightarrow$ 2^n éléments de 0 à $2^n - 1$

Préliminaire: code ASCII (étendu)



ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Extended ASCII characters

128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	ú	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134	å	166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	þ
136	ê	168	¿	200	╚	232	Þ
137	ë	169	®	201	╔	233	Ú
138	è	170	¬	202	╩	234	Û
139	ï	171	½	203	╦	235	Ù
140	î	172	¼	204	╠	236	ý
141	ì	173	¡	205	═	237	Ý
142	Ä	174	«	206	╬	238	¯
143	Å	175	»	207	¤	239	´
144	É	176	░	208	ð	240	≡
145	æ	177	▒	209	Ð	241	±
146	Æ	178	▓	210	Ê	242	‗
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	°
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	·
155	ø	187	╗	219	█	251	¹
156	£	188	╝	220	▄	252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	Ì	254	■
159	ƒ	191	┐	223	▀	255	nbsp

$= 2^8 - 1$

Préliminaire: opération XOR $\oplus$ (addition modulo 2)

$$
\begin{array}{r}
01011010111111010101 \\
\oplus\ 11001000101001011\,0 \\
\hline
10010010011100011
\end{array}
$$

⚠ pas de retenues!

$\oplus$	0	1
0	0	1
1	1	0

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

$A \oplus B = B \oplus A$

$A \oplus B \oplus C = (A \oplus B) \oplus C = A \oplus (B \oplus C)$

Clé à usage unique (chiffre de Vernam, 1917)

- Alice veut envoyer un message M
  (M est donné par sa représentation binaire)
- Alice et Bob partagent une clé K
  (K est aussi donnée par sa rep. binaire)
- ⚠ si longueur $(M) = n$, alors il faut que longueur $(K) = n$

Alice : effectue $C = M \oplus K = f(M, K)$

et transmet C à Bob

Bob : $D = C \oplus K$ fait la même chose !

$0 \oplus 0 = 0 \quad 1 \oplus 1 = 0$!

$\oplus$ { $M = 11010111$, $K = 10101010$, $C = 01111101$

$\oplus$ { $C = 01111101$, $K = 10101010$, $D = 11010111 = M$

$$D = C \oplus k = (M \oplus k) \oplus k$$

$$= M \oplus \underbrace{(k \oplus k)}_{= \text{séquence de } 0} = M \quad \checkmark$$

$$A \oplus B = A \ominus B \quad !!$$

Clé à usage unique: sécurité

Eve : connaît C, mais pas K

⚠ Alice et Bob doivent choisir K ainsi :

- chaque bit K_i doit être tiré uniformément au hasard : $P(K_i = 1) = P(K_i = 0) = \frac{1}{2}$
- tous les bits doivent être tirés indépendamment
- la clé K doit être indépendante de M

Eve : $C = M \oplus K$

$$P(C_i = 0) = P(M_i \oplus K_i = 0)$$

$$= P(M_i = K_i) = P(K_i = M_i) = \frac{1}{2}$$

$$P(C_i = 1) = P(M_i \neq K_i) = \frac{1}{2}$$

(M_i : 0 ou 1)

Donc pour Eve, la séquence C est une séquence de bits très uniformément au hasard!

Clé à usage unique: quiz!

Question 1:

Pourquoi une attaque par force brute ne permettrait-elle pas de casser le système de clé à usage unique (en supposant qu'Eve dispose de la puissance de calcul nécessaire pour essayer toutes les clés possibles) ?

Clé à usage unique: quiz!

Question 2: (reliée à la précédente)

Vu que la clé K est tirée au hasard, il y a une probabilité (petite, certes, mais non-nulle) que tous les bits de K valent exactement 0. Dans ce cas, le message chiffré C est égal au message d'origine M : est-ce grave ?

en pratique : le nombre de 0 de la clé K est entre $\left[\frac{n}{2} - \sqrt{n}, \frac{n}{2} + \sqrt{n}\right]$

Une clé non-réutilisable (comme son nom l’indique…)

Plusieurs messages :

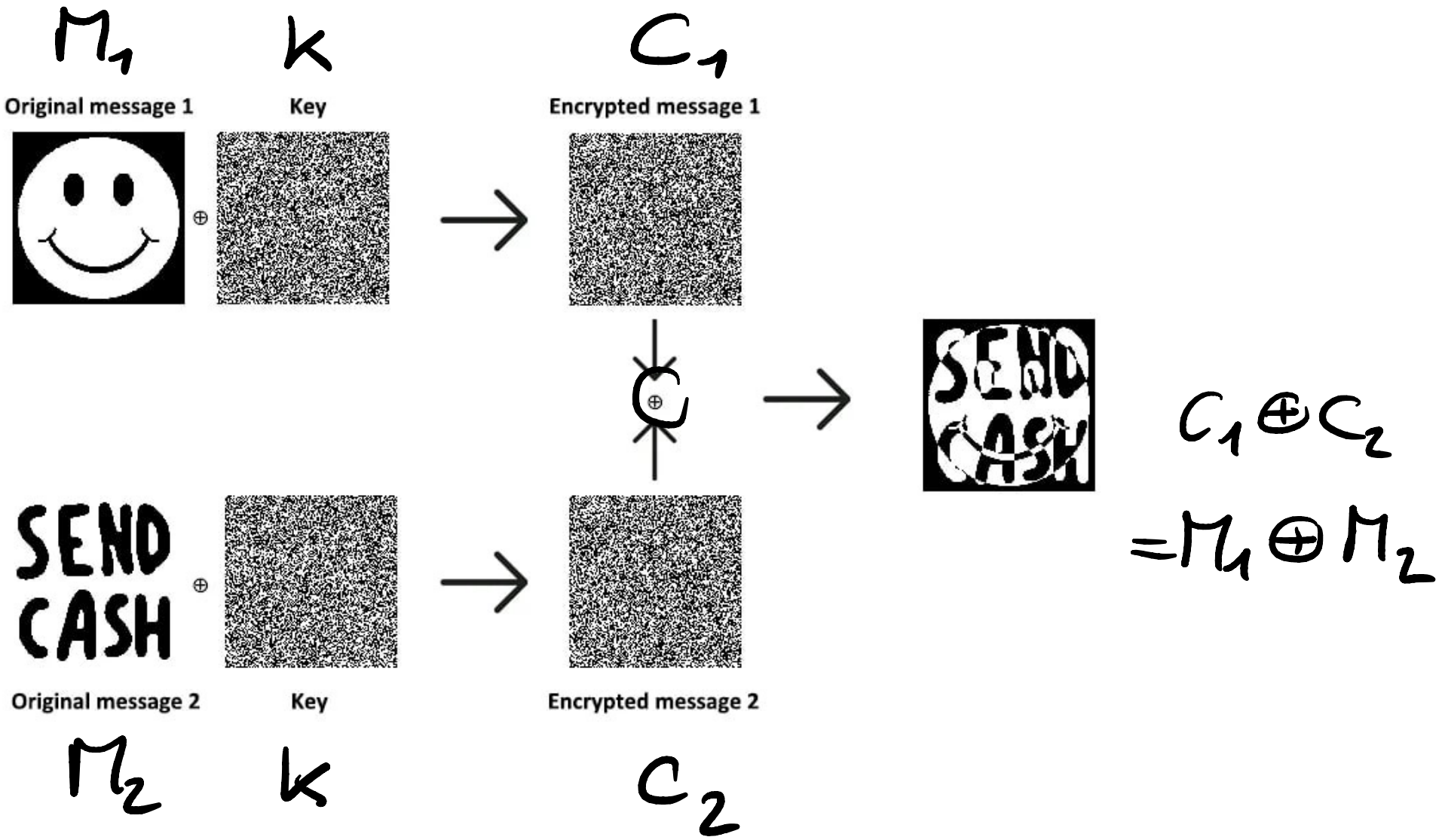
Alice envoie $\begin{cases} C_1 = M_1 \oplus k \\ C_2 = M_2 \oplus k \end{cases}$

Eve : effectue $C_1 \oplus C_2$

$= (M_1 \oplus k) \oplus (M_2 \oplus k) = (M_1 \oplus M_2) \oplus \underbrace{(k \oplus k)}$

$= M_1 \oplus M_2$ la clé k disparaît ! $= 0$

Une clé non-réutilisable: illustration



Première tentative pour réutiliser la clé K

Alice veut envoyer un message M à Bob

(et ils ont échangé une clé k auparavant)

Alice envoie $\begin{cases} C_1 = M_1 \oplus f(k, M_1) \\ C_2 = M_2 \oplus f(k, M_2) \end{cases}$

si Eve effectue $C_1 \oplus C_2 = M_1 \oplus M_2 \oplus f(k, M_1) \oplus f(k, M_2)$ ✓

mais Bob reçoit $C_1 = M_1 \oplus f(k, M_1) \longrightarrow$?

Deuxième tentative pour réutiliser la clé K

Horst Feistel : Divisons en deux $\begin{cases} M = (M_a, M_b) \\ K = (K_a, K_b) \end{cases}$

hyp : longueur M et K = 2n bits (K_a, K_b : n bits chacun)

Alice calcule successivement (n bits) : et envoie $C = (C_a, C_b)$

$$C_a = \underbrace{M_a}_{n \text{ bits}} \oplus f(\underbrace{K_a}_{n \text{ bits}}, \underbrace{M_b}_{n \text{ bits}}) \quad , \quad C_b = M_b \oplus f(K_b, C_a)$$

Deuxième tentative pour réutiliser la clé K

Alice: $C_a = M_a \oplus f(K_a, M_b)$, $C_b = M_b \oplus f(K_b, C_a)$

Bob effectue successivement :

$$\begin{cases} D_b = C_b \oplus f(K_b, C_a) \\ D_a = C_a \oplus f(K_a, D_b) \end{cases}$$

$$D_b = C_b \oplus f(K_b, C_a) = (M_b \oplus f(K_b, C_a)) \oplus f(K_b, C_a)$$

$$= M_b \oplus (f(K_b, C_a) \oplus f(K_b, C_a)) = M_b$$

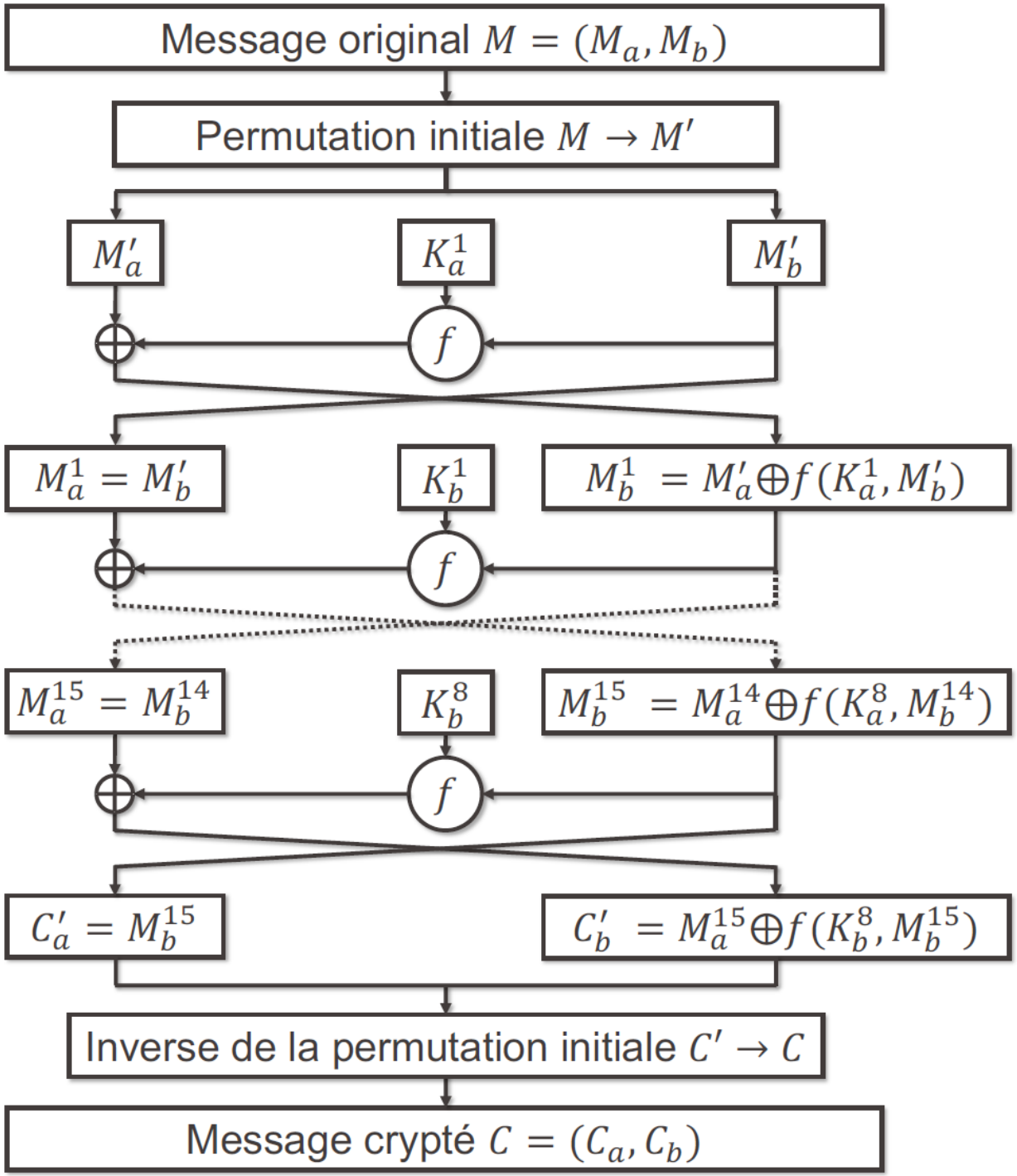
$$D_a = C_a \oplus f(K_a, M_b) = M_a \oplus f(K_a, M_b) \oplus f(K_a, M_b) = M_a$$

Data Encryption Standard (DES, 1977)

Maintenant, on peut réutiliser la clé k de longueur

$2n = 56$ bits

→ AES (clés avec 128, 256 bits)



Sécurité de la clé (attaques par force brute)

56 bits $\longrightarrow$ 2^{56} possibilités $\sim 10^{16}$ abbg. theo. -_-

Mots de passe : avec un alphabet de k symboles et un mot de passe de longueur n

$\longrightarrow$ k^n possibilités

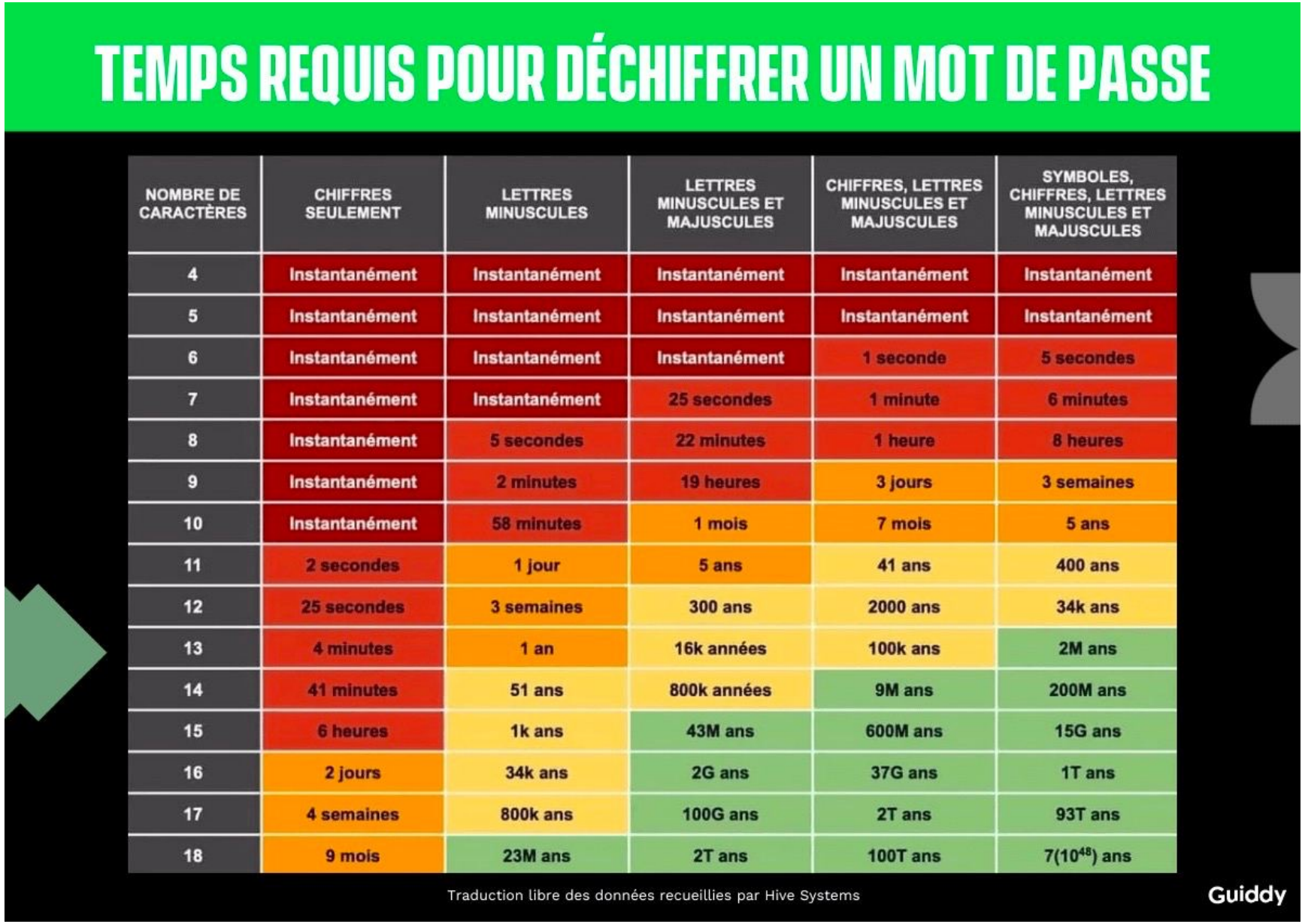
6 chiffres $\longrightarrow$ 10^6 possibilités

15 chiffres : 10^{15} poss

6 lettres maj : $\longrightarrow$ $26^6 \sim 3 \cdot 10^9$ poss.

6 lettres min & maj $\longrightarrow$ $52^6 \sim 2 \cdot 10^{10}$ poss.

Sécurité de la clé



NOMBRE DE CARACTÈRES	CHIFFRES SEULEMENT	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES	SYMBOLES, CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES
4	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
5	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
6	Instantanément	Instantanément	Instantanément	1 seconde	5 secondes
7	Instantanément	Instantanément	25 secondes	1 minute	6 minutes
8	Instantanément	5 secondes	22 minutes	1 heure	8 heures
9	Instantanément	2 minutes	19 heures	3 jours	3 semaines
10	Instantanément	58 minutes	1 mois	7 mois	5 ans
11	2 secondes	1 jour	5 ans	41 ans	400 ans
12	25 secondes	3 semaines	300 ans	2000 ans	34k ans
13	4 minutes	1 an	16k années	100k ans	2M ans
14	41 minutes	51 ans	800k années	9M ans	200M ans
15	6 heures	1k ans	43M ans	600M ans	15G ans
16	2 jours	34k ans	2G ans	37G ans	1T ans
17	4 semaines	800k ans	100G ans	2T ans	93T ans
18	9 mois	23M ans	2T ans	100T ans	$7(10^{48})$ ans

Exercice 1

A utiliser:

a) Il y a deux façons de faire: depuis la gauche ou depuis la droite

b) ord(caractère) = code ASCII étendu de celui-ci $\epsilon \{0, \dots, 255\}$

puis réutiliser la partie a)

[Attention: chaque caractère doit être encodé sur 8 bits!]