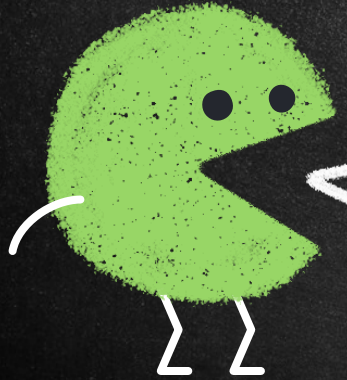
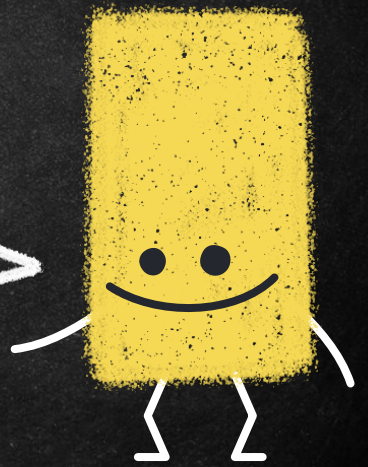
Sécurité des données
A2021

Encryption Symétrique

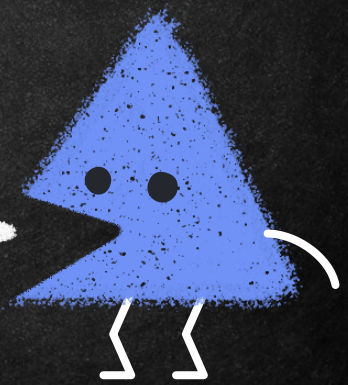




Yannick Charron

Plan de la séance

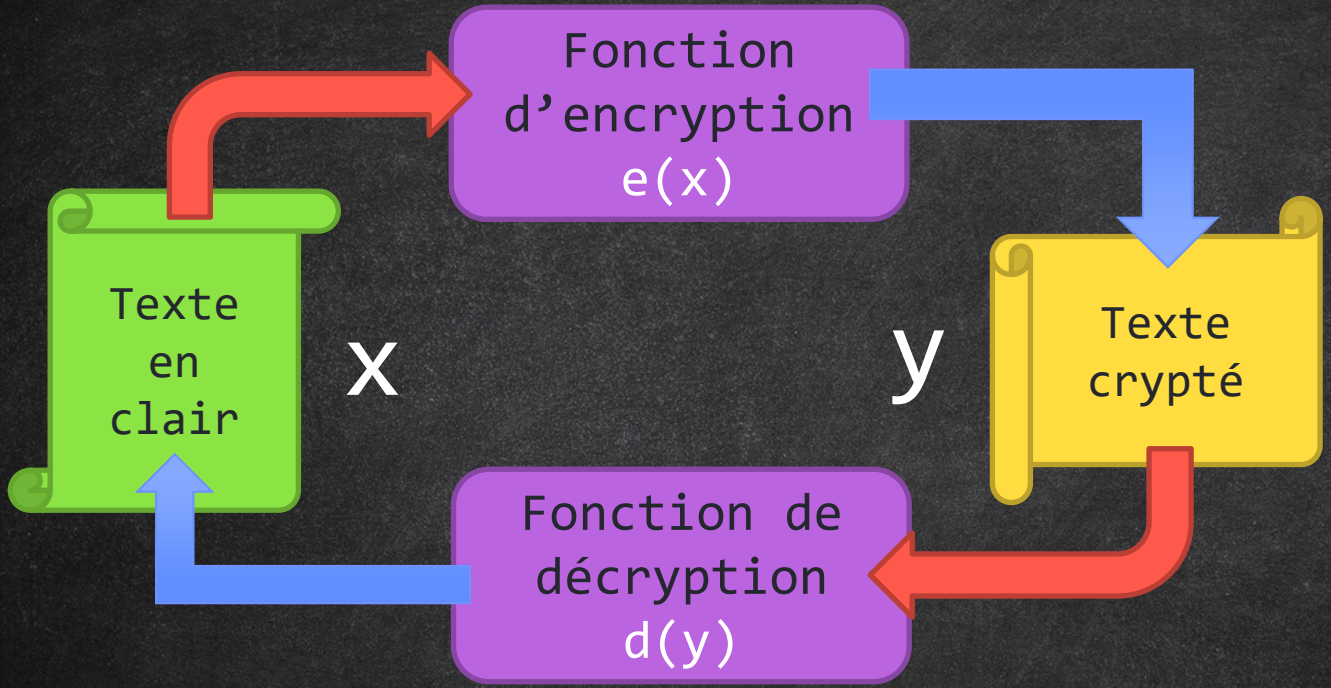
- Concept général
- Encryption simple
- Encryption alphabétique
- Encryption moderne

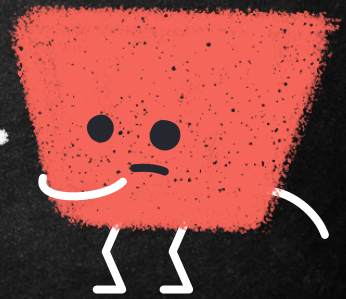


Concept général

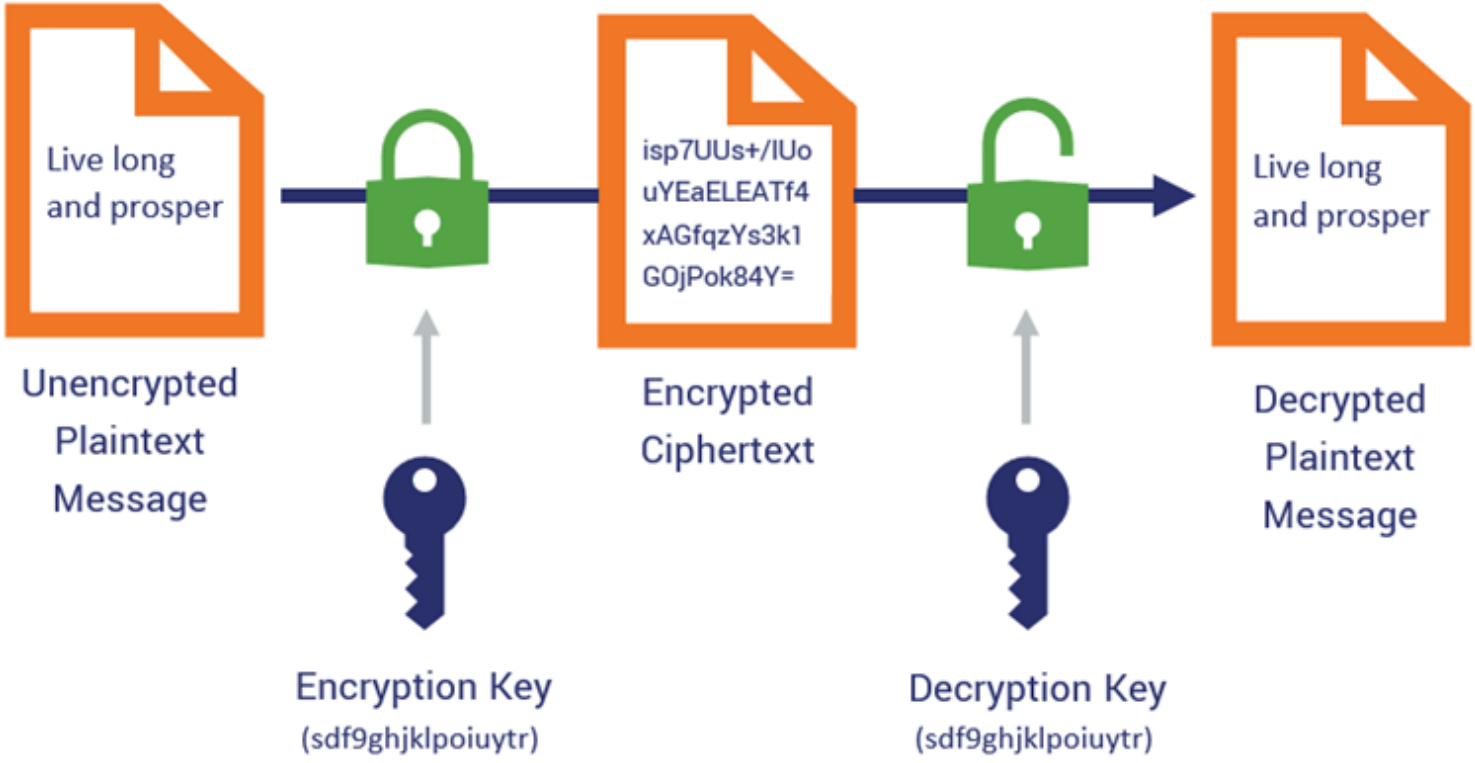
- Protéger le contenu d'un message dans le but de le communiquer
- Permettre à un nombre limité de participant de consulter le contenu du message

Concept Général

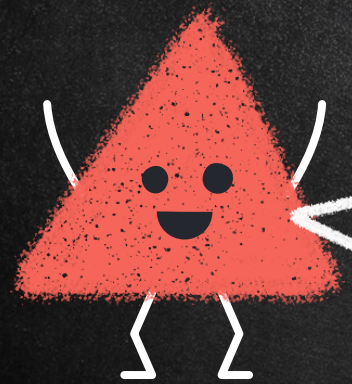


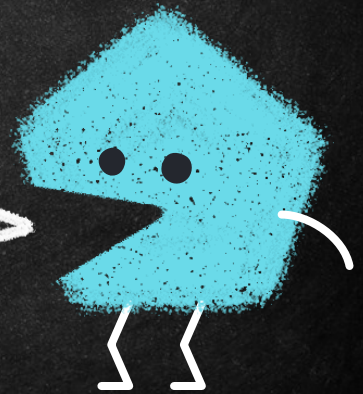


How Symmetric Encryption Works



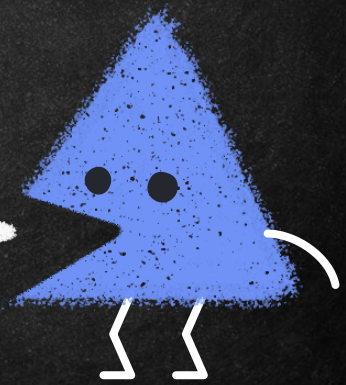
Encryption Simple

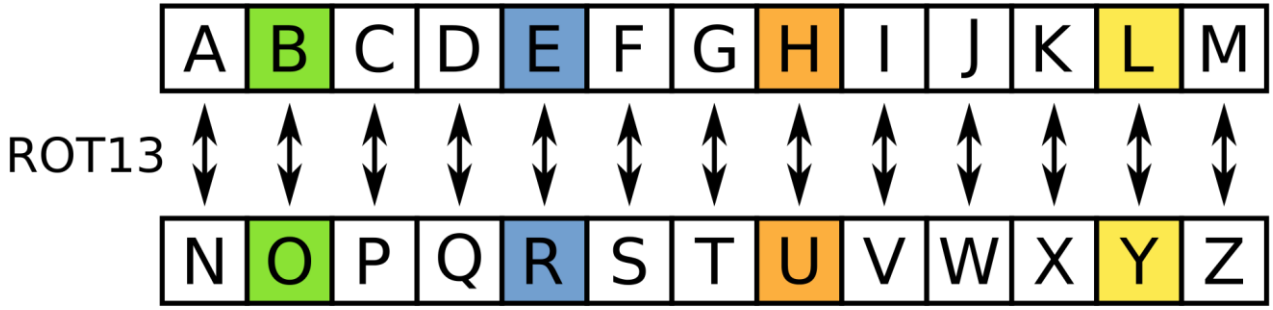


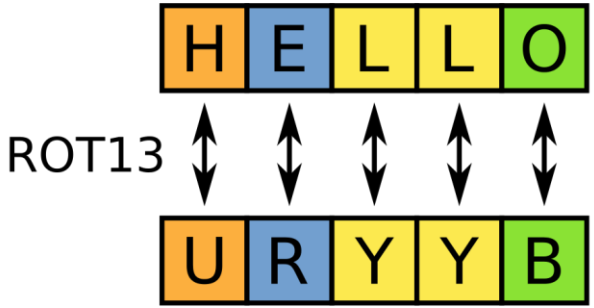


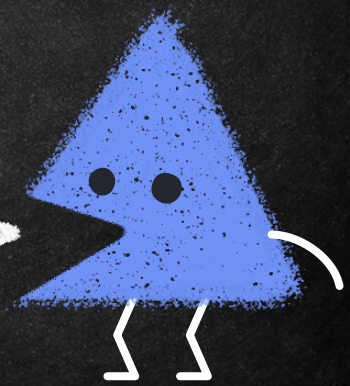
Encryption Monoalphabétique

- Monoalphabétique
  - Code César
  - Rot13




A B C D E F G H I J K L M
ROT13
N O P Q R S T U V W X Y Z

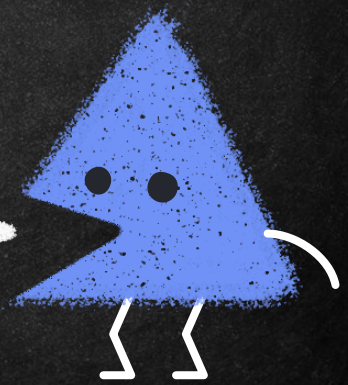

H E L L O
ROT13
U R Y Y B



Encryption polyAlphabétique

- Le décalage n'est pas fixe, il utilise une clé
- Décalage selon le rang de la lettre dans la clé (A = 0)

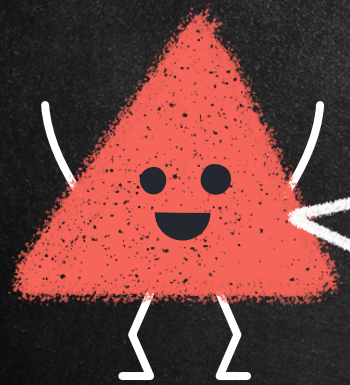
M	O	N		M	E	S	S	A	G	E		S	E	C	R	E	T		U	R	G	E	N	T
C	I	T	R	O	N	C	I	T	R	O	N	C	I	T	R	O	N	C	I	T	R	O	N	C
2	8	19	17	14	13	2	8	19	17	14	13	2	8	19	17	14	13	2	8	19	17	14	13	2

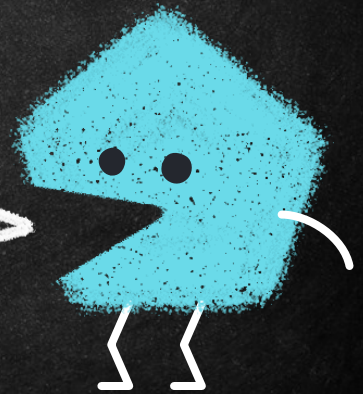


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Égnima

Un mélange de Mono et Poly






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

Geheime Kommandosache! Jeder einzelne Tagesschlüssel ist geheim! Mitnahme im Flugzeug verboten! Nº 000082

Luftwaffen-Maschinen-Schlüssel Nr. 2744

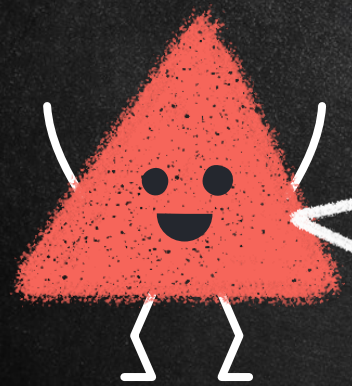
Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

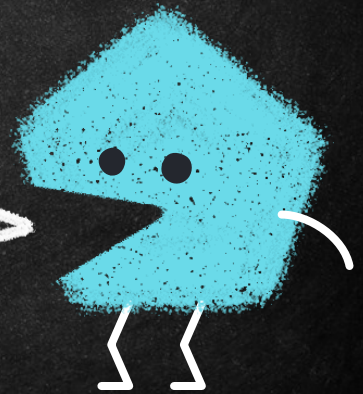
	Monats-Tag	Walzenlage			Ringstellung			an der Umkehrwalze	Steckerverbindungen am Steckerbrett 1	2	3	4	5	6	7	8	9	10	Zusatzstecker-verbindungen 1 (1500)	2 (2300)	Kenngruppen		
2744	31	III	V	IV	17	11	04	TZ UX SV CO EP IM	TW	BI	UY	GP	CK	JQ	DL	RV	EM	AH	NS	FO	kim	pwh	sbx	csw
2744	30	I	IV	V	08	17	21		LS	DH	MT	EO	AP	UZ	FQ	WY	BK	GR	CI	JN	uaq	omn	ume	duf
2744	29	V	II	III	11	14	05		DO	JW	CN	IV	PZ	BM	HU	AL	FR	KX	EQ	GT	don	cqo	xum	bpg
2744	28	II	IV	V	02	20	16		NT	HK	BW	EP	LQ	AU	OY	FJ	CX	GI	DZ	MR	lui	pyg	sby	dtq
2744	27	III	V	IV	18	13	22		HM	GV	KZ	AI	DQ	NR	ES	BL	OU	FT	CP	JY	cmy	fqr	scl	bur
2744	26	I	III	II	24	10	01		GW	AQ	MO	FV	PS	DI	RU	JZ	BN	EH	KT	CL	kbj	yaq	udm	cnz
2744	25	IV	I	III	04	25	23		LT	DR	QX	AG	IN	EU	BJ	KP	FW	CM	SZ	HO	kqz	yar	vdb	coa
2744	24	V	III	I	09	19	06		GL	MY	CR	HN	JX	DT	AF	PU	IQ	BO	EW	KS	cmz	aoj	zod	auh
2744	23	IV	I	V	15	03	19	HK GL NQ BF AD RW	IT	DV	HQ	AJ	MU	EX	KO	CS	FY	LN	BP	GZ	kra	yas	xun	cob
2744	22	I	V	III	12	26	07		EY	JL	AK	NV	FZ	CT	HP	MX	BQ	GS	DW	IO	jdm	uhf	xuo	bph
2744	21	III	IV	II	15	09	12		JP	DY	QS	HL	AE	NW	CU	IK	FX	BR	MV	GO	jpf	aok	iys	btx
2744	20	IV	II	I	02	22	05		HT	NP	AM	DX	GJ	KQ	BS	OV	ER	CW	IU	FL	boy	wac	uow	cse
2744	19	V	I	II	08	19	17		GM	OX	BT	QU	DP	HJ	FK	SW	AN	EL	CY	IR	xjc	wad	unj	ctd
2744	18	III	IV	I	11	21	01		KW	IP	DM	SV	JR	CX	EN	AZ	QT	BU	FH	GY	kpn	rzi	vcm	bpo
2744	17	I	V	II	18	23	14		BV	HW	AR	NX	DS	PT	CZ	FI	LY	EJ	GK	MQ	kdx	crq	vcn	cod
2744	16	III	IV	V	16	04	07		LU	CV	FM	KR	BY	GN	QW	DJ	PS	AO	EI	HX	lgx	jri	uob	aur
2744	15	V	III	IV	24	13	10		HZ	NQ	AD	TV	IX	KM	BG	LO	CE	RY	JU	FP	wpt	vhy	zoe	aus
2744	14	I	IV	II	06	20	25		FN	UY	CJ	IW	LP	AS	DK	GQ	MO	BZ	ET	HR	wog	hxi	zxi	bpi
2744	13	III	II	I	03	26	18		KR	IZ	AT	NV	BH	MP	CG	OY	ES	DF	UW	LQ	lqv	iqb	zsy	coe
2744	12	II	IV	III	04	11	15		DT	JV	HS	CI	AY	KU	EN	FQ	LR	BW	MP	GO	zic	myt	zof	dtr
2744	11	V	I	IV	16	07	02		JS	PW	AV	QX	DN	IZ	KM	CO	EG	FL	HY	BR	inf	zbm	krz	dug
2744	10	IV	III	II	20	12	14		FS	CQ	JO	PR	AW	HV	EZ	KN	DU	GT	IL	BY	ink	acu	zxj	cnu
2744	9	III	II	V	06	18	10		HK	TZ	MX	LW	GQ	AD	NY	BE	CS	JP	RV	IO	efm	pmi	snw	cof
2744	8	V	I	III	01	21	17		GU	SW	BF	RX	EV	OT	LQ	CH	IP	KY	JM	NZ	imy	rjw	tjm	cog
2744	7	II	V	I	25	08	23		CX	AZ	DV	KT	HU	LW	GP	EY	MR	FQ	IN	OS	inv	rkc	snx	bpj
2744	6	IV	II	V	13	26	03		DV	LP	NQ	GZ	OS	FK	EW	MR	IT	HX	UY	BJ	yvu	hsb	swq	aut
2744	5	III	I	II	24	19	22		SY	EK	NZ	OR	CG	JM	QU	PV	BI	LW	TX	DF	seu	iqe	swr	auv
2744	4	II	IV	I	17	05	09		BD	GV	AX	KP	EM	FN	CW	RU	HO	JT	IL	QS	zfj	hxj	zxk	dpt
2744	3	V	II	IV	20	16	11		JT	NW	DU	EO	KV	BY	FS	HQ	IM	LX	GP	CR	clx	zbn	zxa	buk
2744	2	II	III	V	14	03	19		RW	OQ	GI	AZ	EJ	MS	CU	DH	PY	BF	LV	TX	ljs	jre	zpq	coh
2744	1	III	I	IV	18	24	15	HL KN FM EI AC BG DS OW PZ QX RU TV	NF	JV	LY	IX	KQ	AO	DZ	CR	FT	EM	GS	HW	plf	dgw	tjn	cnv

Diese Zusatzsteckerverbindungen ersetzen zu den angegebenen Zeiten die Steckerverbindungen 1 und 9


ENIGMA,
LE CODE
PARFAIT ?

Encryption symétrique



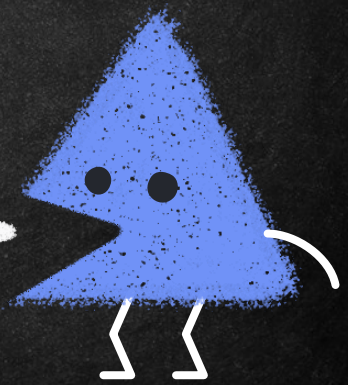


Algorithmes

- Data Encryption Standard (DES)
  - Triple DES
- RC
- Rijndael algorithm family (AES)
- Autres
  - Domaine de l’internet de objet

Vocabulaire

- Cipher et Decipher
- Clé:
- iv: Initialization vectors



Clé d'encryption ou secret

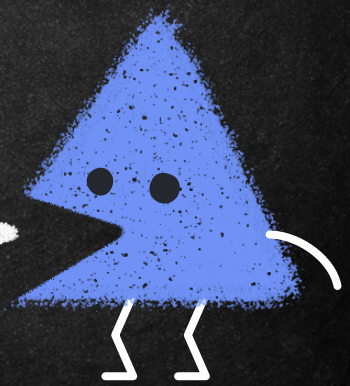
- Seulement une clé d'encryption
- Chaque partie prenante de la communication doit avoir le même secret

Algorithmes connus

DES	RC
Début 1970 Norme en 1977 Clé de 56 bits 1990: protection faible	RC2 et RC4 :1987 Clé de 40 bits Ne sont plus considéré sécuritaire RC5 Clé jusqu'à 2040 bits Sécurité vs Performance Brevet …
Triple DES	
3 clés d'encryptions	

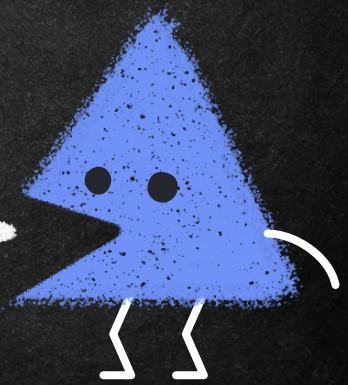
Advanced Encryption Standard

- 2001
- 3 tailles de clé (128, 192, 256 bits)
- Protection de niveau militaire
- Avec une clé de 128 bits
  - Milliards d’année pour briser avec un ordinateurs classique



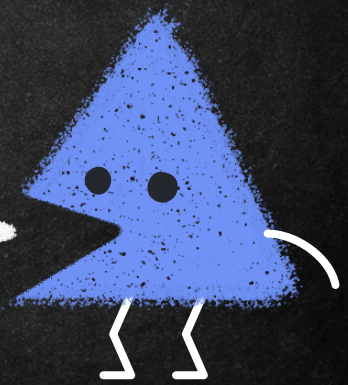
Informatique Quantique

- L’effet sur AES aura pour effets de diviser la longueur de clé par deux
- Donc AES-256 devrait toujours être sécuritaire
- L’encryption asymétrique sera néanmoins compromise

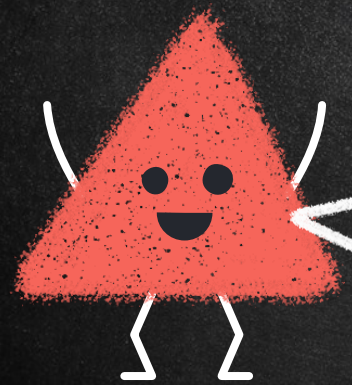


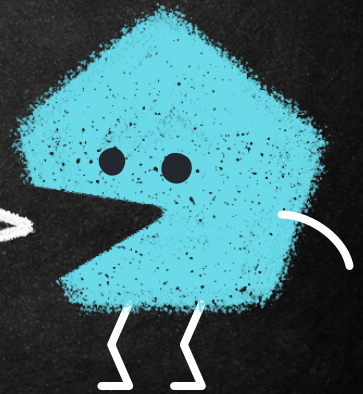
LIGHTWEIGHT

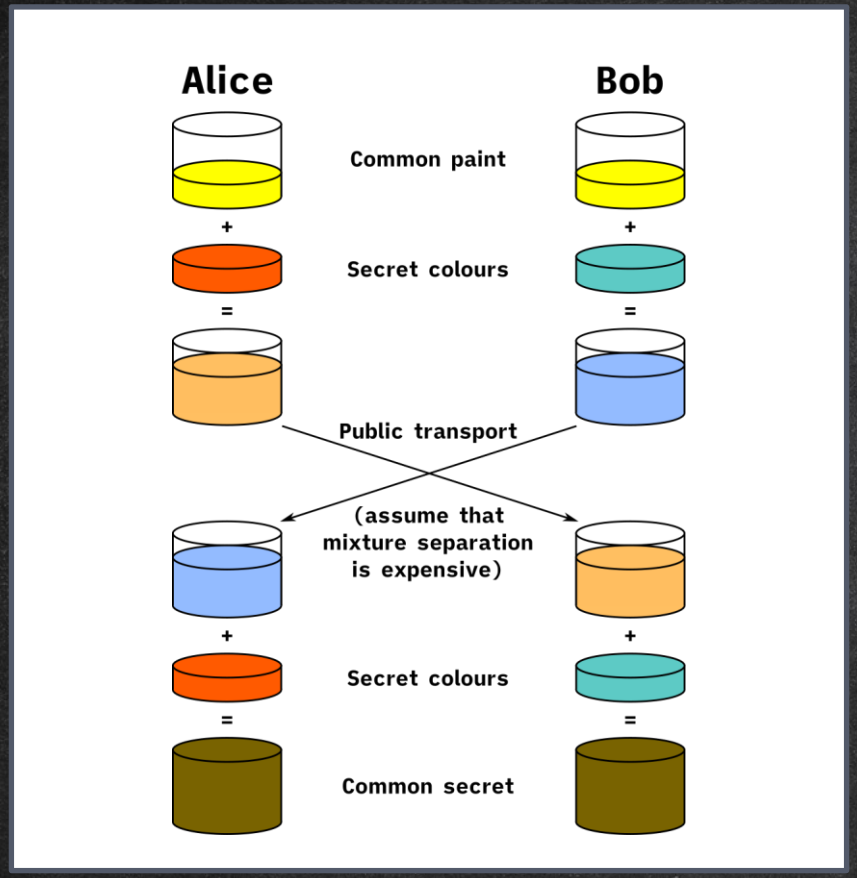
- Les recherches sont en cours
- Internet des objets
- https://csrc.nist.gov/projects/lightweight-cryptography



Diffie-Helleman






Alice
Bob
Common paint
+
Secret colours
=
Public transport
(assume that
mixture separation
is expensive)
+
Secret colours
=
Common secret