Cryptographie Moderne et Appliquée

Dr Salim Benayoune

Plan du cours

- Introduction
- Cryptographie symétrique
  - Cryptographie par **flot continu**
  - Cryptographie par **bloc**
    - DES, 3-DES, AES
  - Modes opératoires
- Cryptographie asymétrique
  - RSA
  - Diffie Hellman
  - Signature numérique
- Fonctions de hachage
- Méthodes d'authentification
- Exemples : TLS, PKI, SSH, WPA, Bitcoin

INTRODUCTION

La cryptographie est partout

Communication sécurisée :

Trafic web : HTTPS, SSH, IPsec

trafic sans fil: 802.11i WPA2, 4G/5G, Bluetooth

Chiffrement des fichiers sur le disque: EFS, TrueCrypt, bitlocker

Cryptomonnaie

Authentification de l'utilisateur

… et bien plus encore

Cas d’usage

Clé à usage unique : (clé à usage unique)

La clé n’est utilisée que pour chiffrer un seul message

- email

Clé multi-usage: (clé à usage multiple)

Clé utilisée pour chiffrer plusieurs messages

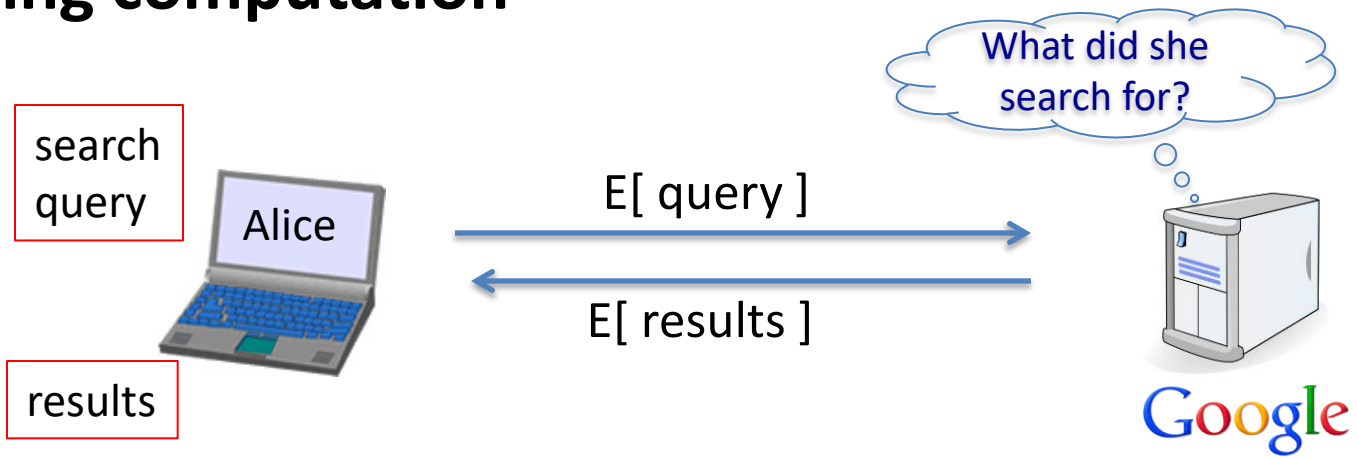
- fichiers cryptés: même clé utilisée pour chiffrer de nombreux fichiers

Autres Usages

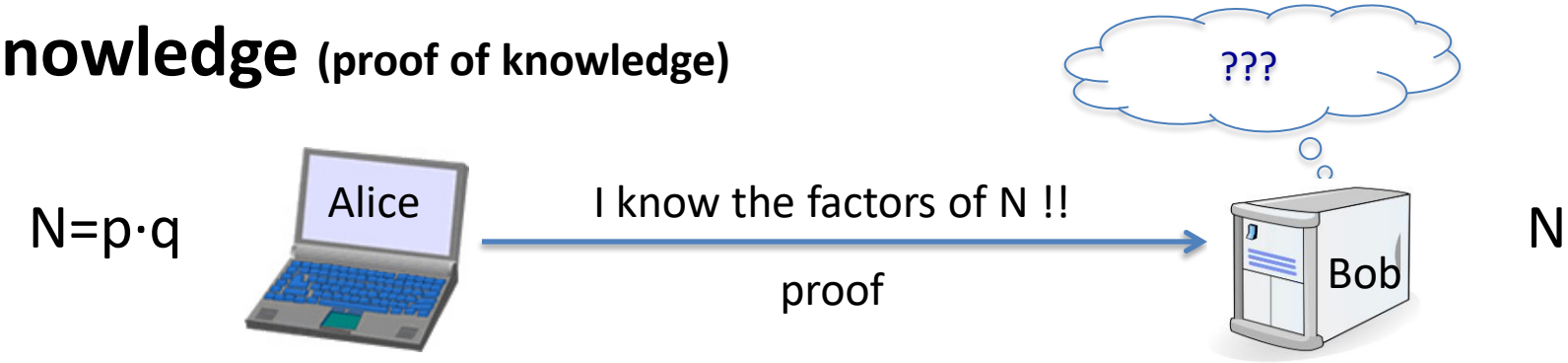
- Signatures numériques
- Communication anonyme
- Monnaie numérique anonyme
  - Puis-je dépenser de l'argent sans que personne ne sache qui je suis ?
  - Comment éviter les **doubles dépenses** ?
- Election privée
- Enchère

Autres Usages

- **Privately outsourcing computation**



- **Zero knowledge (proof of knowledge)**



Une science rigoureuse

Les trois étapes de la cryptographie :

- Spécifier avec précision le **modèle de menace**
- Proposer une **construction**
- Prouvez que briser la construction résoudra un problème difficile sous-jacent

Choses à retenir

- La cryptographie, **c'est** :
  - Un outil formidable
  - La base de nombreux mécanismes de sécurité

- La cryptographie **n'est pas** :
  - La solution à tous les problèmes de sécurité
  - Fiable à moins d'être implémentée et utilisée correctement
  - Quelque chose que vous devriez essayer d'inventer vous-même
    - de nombreux exemples de conceptions ad hoc cassées

Chiffre de césar

- Par **substitution**

```
plain:  meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$C = E(k, p) = (p + k) \; mod \; 26$$

$$p = \mathrm{D}(k, C) = (C - k) \bmod 26$$

Cryptanalyse et attaque par force brute

- **Cryptanalyse :**
  - Repose sur la **nature de l'algorithme** et peut-être sur une certaine connaissance des caractéristiques générales du texte en clair ou même sur des exemples de paires texte clair-texte chiffré.

- **Brute force :**
  - L'attaquant essaye toutes les clés possibles jusqu'à ce qu'une traduction intelligible en texte clair soit obtenue. **En moyenne**, la moitié de toutes les clés possibles doivent être essayées pour réussir.

Analyse du chiffre de César

- Trois caractéristiques importantes de ce problème nous ont permis d'utiliser la force brute :

1. Les algorithmes de chiffrement et de déchiffrement sont connus.
2. Il n'y a que **25** clés à essayer.
3. La langue du texte brute **est connue** et facilement reconnaissable.

```
PHHW PH DIWHU WKH WRJD SDUWB
KEY
1 oggv og chvgt vjg vqic rctva
2 nffu nf bgufs uif uphb qbsuz
3 meet me after the toga party
4 ldds ld zesdq sgd snfz ozqsx
5 kccr kc ydrcp rfc rmey nyprw
6 jbbq jb xcqbo qeb qldx mxoqv
…..
```

Chiffrement mono-alphabétique

- Une **permutation** d'un ensemble fini d'éléments **S** est une suite ordonnée de tous les éléments de **S**, chaque élément apparaissant exactement une fois.

- Exemple :

$$S = \{a, b, c\} : \quad P = \{abc, acb, bac, bca, cab, cba\}$$

$$|\boldsymbol{S}| = \boldsymbol{n} \Rightarrow |\boldsymbol{P}| = \boldsymbol{n}!$$

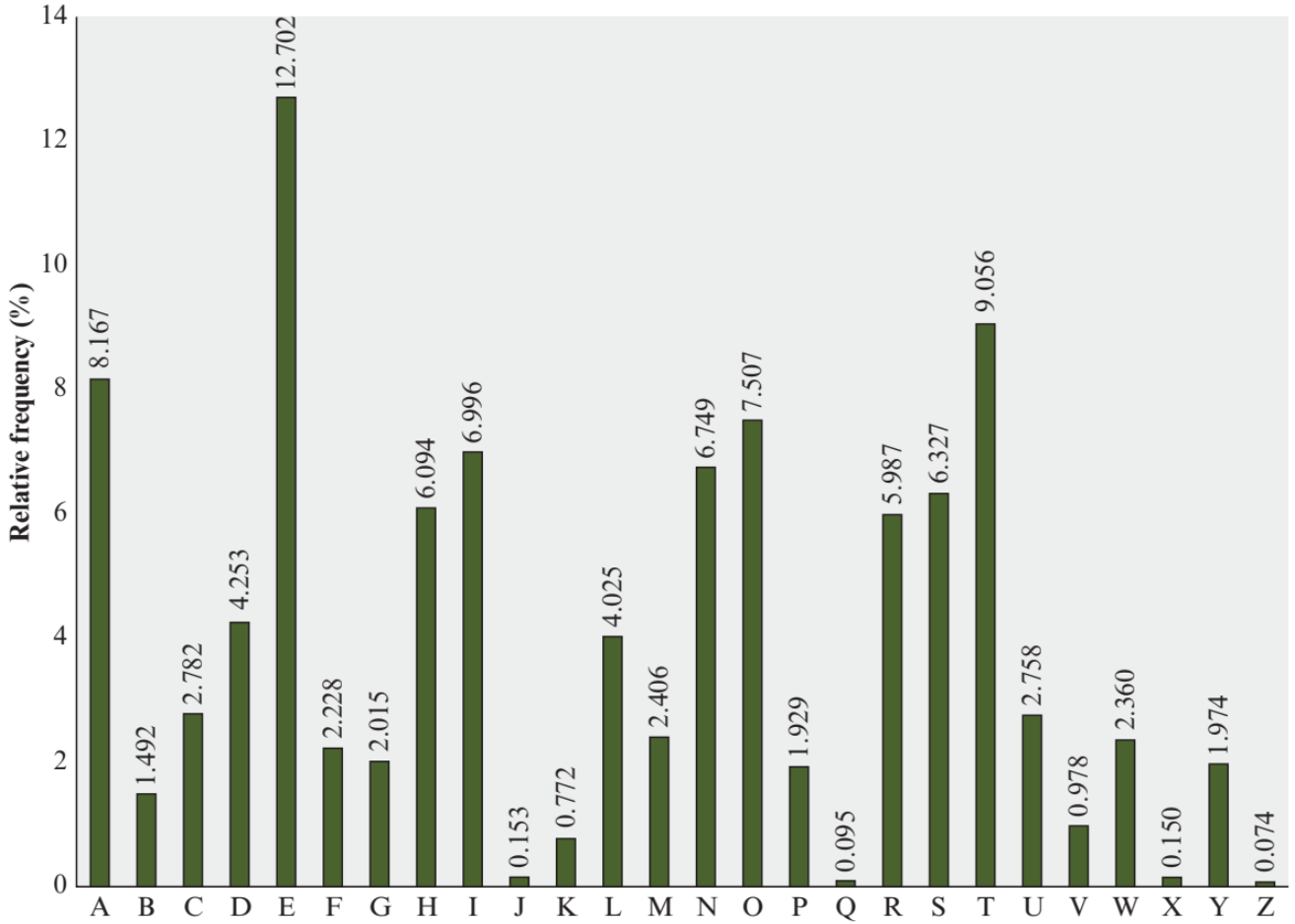
Plaintext alphabet	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext alphabet	GOYDSIPELUAVCRJWXZNHBQFTMK

- Si la ligne Cipher peut prendre n'importe quelle permutation, il y aura **26!** Permutations:

$$26! \approx 4.03 \cdot 10^{26} \approx 2^{88}$$

Chiffrement Monoalphabétique

- Cryptanalyse fréquentielle



Exemple

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYYFVUFOFEIKNWFRFIKJNUPWRFIPOUNVNIPU
BRNCUKBEFWWFDNCHXCYBOHOPYXPUBNCUBOYNRVNIWNCPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCY
ZPUKBZPUNVPWPCYVFZIXUPUNFCPWRVNBCVBRPYYNUNFCPWWJUKBYBIPOUZBCUIPOUNVNIPUBRNCHOPYXPUBNCUBOYNRVNIWNC
POJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZPUNVR

B	36
N	34
U	33
P	32
C	26

➔ E

➔ T

➔ A

NC	11
PU	10
UB	10
UN	9

digrams

➔ IN

➔ AT

UKB	6
RVN	6
FZI	4

trigrams

➔ THE

- Solution au problème :
  - Chiffrer plusieurs lettres à la fois
  - Utiliser plusieurs alphabets

Chiffres de substitution polygrammiques

- Dans les systèmes polygrammiques, un groupe de **n** lettres est chiffré par un groupe de **m** symboles.

- Les lettres ne sont donc pas chiffrées séparément, mais par groupes. On parle parfois de **chiffrement par blocs**.

Chiffres de substitution polygrammiques

❑ Playfair

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

Règle 1

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

Règle 2

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

Règle 3

- **Règle 1 :** Si les deux lettres sont sur les coins d'un rectangle, alors les lettres chiffrées sont sur les deux autres coins.
- **Règle 2 :** Si deux lettres sont sur la même ligne, on prend les deux lettres qui les suivent immédiatement à leur droite
- **Règle 3 :** Si deux lettres sont sur la même colonne, on prend les deux lettres qui les suivent immédiatement en dessous
- **Règle 4:** Si le bigramme est composé d'une lettre répétée, on insère une nulle (usuellement le X) entre les deux pour éliminer ce doublon.

Chiffrement polyalphabétique

- Utiliser plusieurs alphabets :

Plaintext alphabet	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext alphabet one	TMKGOYDSIPELUAVCRJWXZNHBQF
Ciphertext alphabet two	DCBAHGFEMLKJIZYXWVUTSRQPON

  - Question: chiffrer le mot « tester »

Chiffrement polyalphabétique

- Chiffrement de Vigenère

k = C R Y P T O C R Y P T O C R Y P T

(+ mod 26)

m = W H A T A N I C E D A Y T O D A Y

---

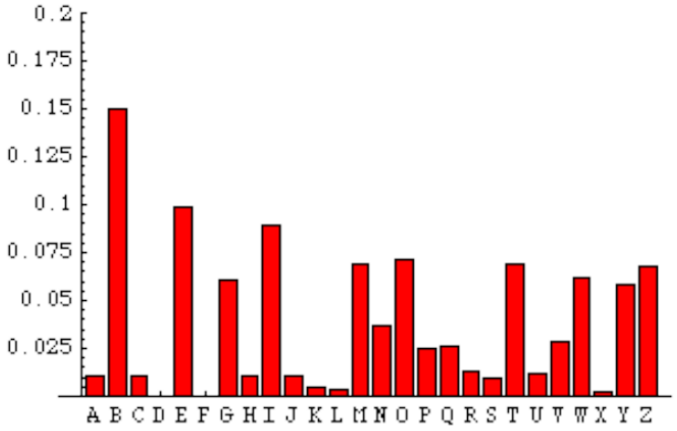
c = Z Z Z J U C L U D T U N W G C Q S

- Comment décrypter ?

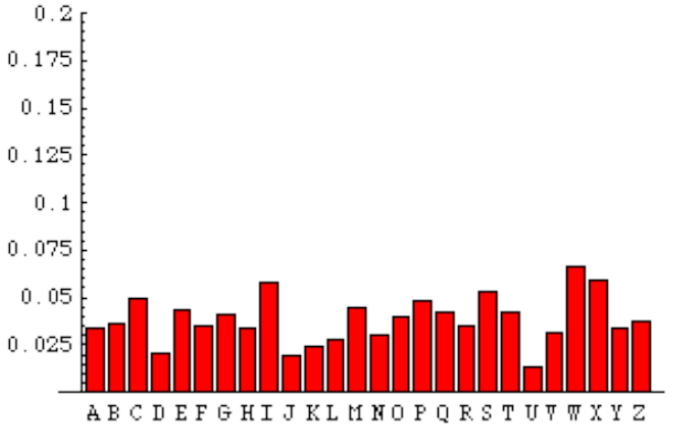
Chiffrement de Vigenère

- Utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message

Clair	c	h	i	f	f	r	e	d	e	v	i	g	e	n	e	r	e
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

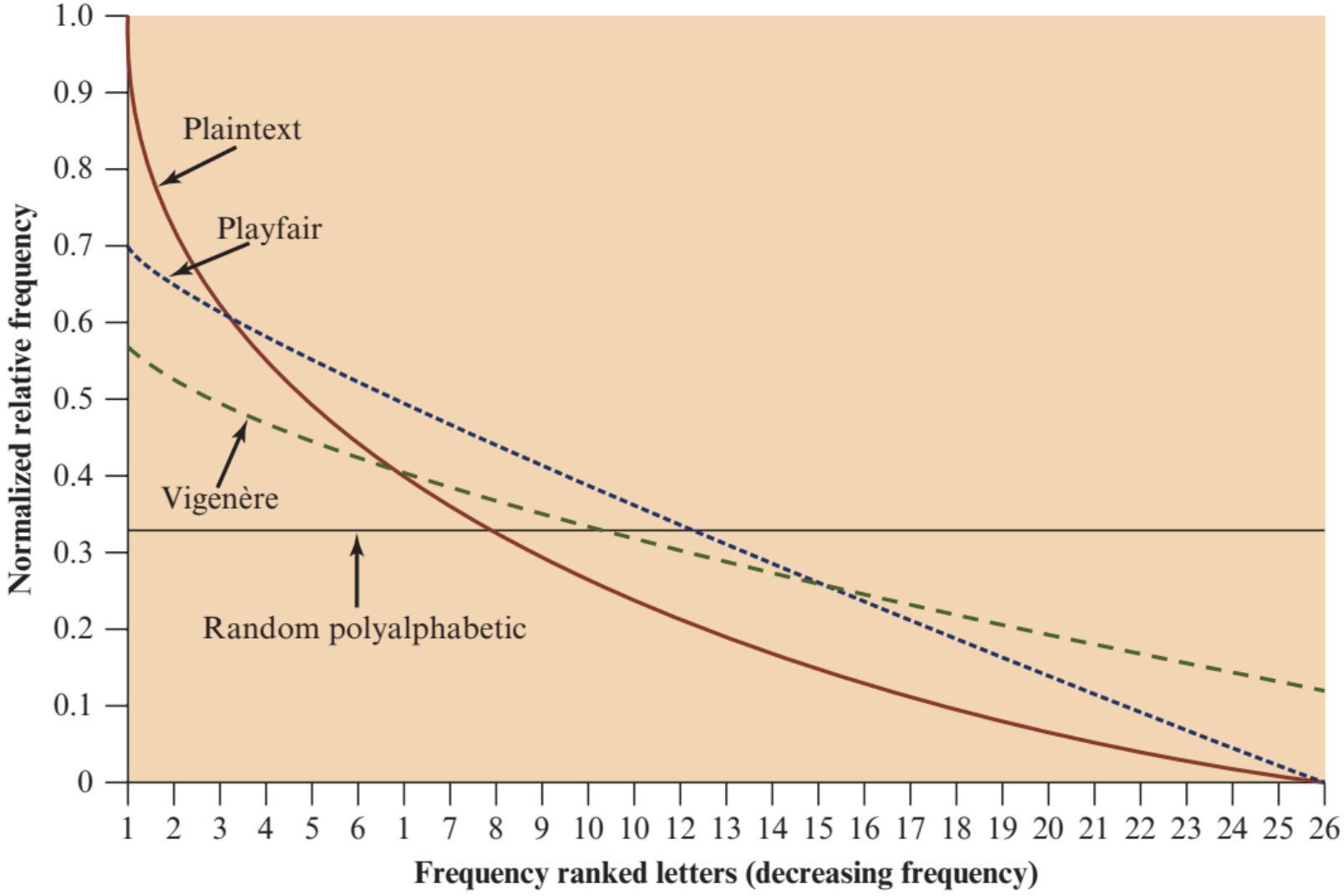


Substitution simple



Chiffre de Vigenère

Fréquences


1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Normalized relative frequency
Plaintext
Playfair
Vigenère
Random polyalphabetic
1 2 3 4 5 6 1 7 8 9 10 10 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Frequency ranked letters (decreasing frequency)

Machines à Rotors

Enigma **(3-5 rotors)**

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EKMFLGDQVZNTOWYHXUSPAIBRCJ
AJDKSIRUXBLHWTMCQGZNPYFVOE
BDFHJLCPRTXVZNYEIWGAKMUSQO
ESOVPZJAYQUIRHXLNFTGKDCMWB
VZBRGITYUPSDNHLXAWMJQOFECK
```

Principe d'Auguste Kerckhoffs (1883)

- La difficulté du déchiffrement ne doit pas dépendre du secret des algorithmes mais du secret des clés

- Autrement dit, il faut supposer l'algorithme complètement connue de l'attaquant, seule la clé utilisée reste secrète
  - Les algorithmes secrets ne le restent souvent pas très longtemps (exemple: RC4), et on leur découvre alors souvent des faiblesses structurelles
  - Il vaut mieux entreprendre cette analyse avant!

Le masque jetable (One Time Pad)

- Tous les crypto-systèmes **sauf un** sont vulnérables si l'attaquant dispose de suffisamment de ressources de calcul

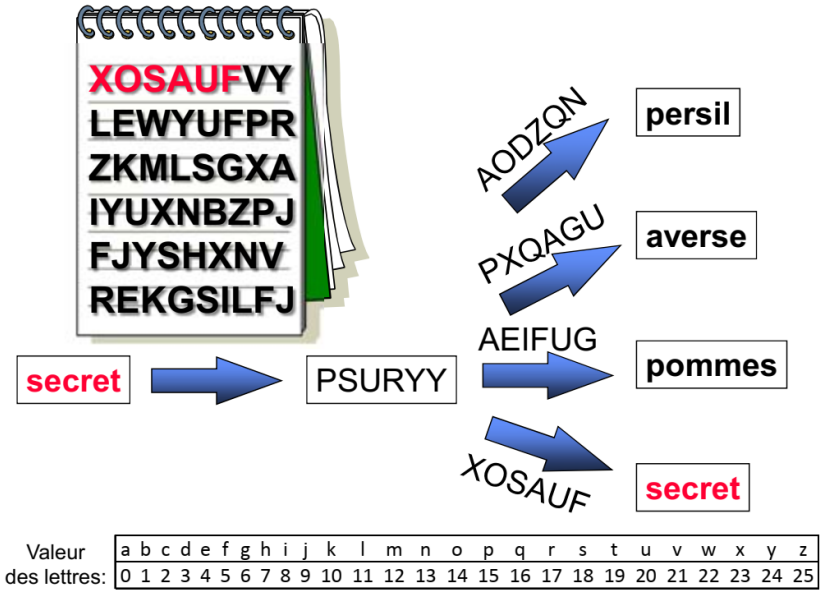
- Un seul algorithme offre **une sécurité inconditionnelle** : le masque à usage unique ('one-time pad') ou chiffre de Vernam
  - Inventé en 1917 par Robert Vernam chez AT&T
  - Joseph Mauborgne a l'idée de la clé à usage unique en 1920
  - Claude Shannon a démontré en 1949 que cet algorithme est incassable

Le masque jetable (One Time Pad)

- On utilise une liste **très longue et aléatoire** de caractères comme clé de chiffrement.
- Chaque caractère est utilisé **une seule fois** pour chiffrer exactement un caractère du texte à transmettre.
- Le destinataire dispose **de la même liste** de caractères pour déchiffrer le cryptogramme transmis.
- Immédiatement après son utilisation, chaque extrémité **détruit** irrémédiablement la portion de la liste utilisée.

Le masque jetable (One Time Pad)

- Pour un message chiffré C, quelque soit le message en clair M, il existe une clé K telle que M ⊕ K = C. Alors, on ne peut rien savoir sur le contenu du texte en clair.



- Les ordinateurs du futur (quantique ou non) ne pourront jamais casser cet algorithme.

Limitations du masque jetable

- La clé (masque) doit être aussi longue que tous les messages à chiffrer réunis !
- Le masque doit être **réellement aléatoire** : fabriqué par lancement d'un dé à 26 faces
- Le masque doit être **transmis de façon sécurisée** entre les deux protagonistes
  - Espion partant en mission, valise diplomatique…
- Algorithme utilisé pour les canaux de communication ultraconfidentiels à faible débit : espions russes, « téléphone rouge » (télex) entre Moscou et Washington…

Conclusion

- Les mots de passe et les clés de chiffrement sont les seules données numériques qui s'usent au fur et à mesure qu'on les utilise :
  - Une répétition minimale des clés utilisées procure une plus grande résistance à la cryptanalyse
  - Le volume de trafic chiffré avec un même jeu de clés conditionne le niveau de sécurité atteint : plus on réutilise une clé, plus le cryptanalyste a des chances de repérer un motif ou des répétitions qu'il pourra exploiter
  - Plus on dispose d'information sur l'émetteur, plus on peut déterminer facilement le contenu d'un message
  - Même s'il est théoriquement sûr, la sécurité d'un cryptosystème peut être anéantie par le non-respect de ses consignes d'utilisation : la discipline des utilisateurs est primordiale.