Mathématiques-Cryptographie

Anne Garcia-Sanchez

M2i cyber2 dev - CFA CCI Avignon

22 février 2024

Chiffrement de Vernam

Chiffre de Vernam - Chiffre à masque jetable - One time pad (OTP)

1917: ingénieur américain Gilbert Vernam

alphabet: n lettres

clé de chiffrement: suite de nombres **aléatoires et indépendants**, compris entre 0 et $n-1$.

message chiffré: décalage de chaque lettre du message clair par le nombre donné par la clé comme dans le chiffre de Vigenère.

Chiffrement de Vernam

Exemple: on chiffre le mot MESSAGE avec la clé HZOZGFL

clé	H	Z	O	Z	G	F	L
message clair	M	E	S	S	A	G	E
rang lettre du message	12	4	18	18	0	6	4
rang lettre de la clé	7	25	14	25	6	5	11
somme rangs	19	29	32	43	6	11	15
réduction modulo 26	19	3	6	17	6	11	15
message chiffré	T	D	G	R	G	L	P

Chiffrement parfait

Un système de chiffrement est dit **parfait** si la connaissance d'un message chiffré n'apporte absolument aucune information sur le message clair même pour un attaquant ayant des outils infiniment puissants à sa disposition.

Chiffrement de Vernam: chiffrement parfait

Claude Shannon a prouvé en 1949 que ce chiffrement est **parfait** si:

- clé: suite de caractères au moins aussi longue que le message à chiffrer.
- clé choisie de façon totalement aléatoire,
- clé utilisée une seule fois.

Chiffrement de Vernam: messages binaires

opération bit à bit de *ou exclusif* ou *xor* noté $\oplus$

correspond à l'addition modulo 2 pour chaque bit

texte clair:	011010000110010101101100011011000110111
clé:	011000101001001001001010101101010010111
texte chiffré:	000010101111011100100110110110010100001

Chiffrement de Vernam: messages binaires

m message clair
k clé de chiffrement
c message chiffré

Chiffrement:

$$c = m \oplus k$$

Le déchiffrement s'obtient aussi par *ou exclusif* car

$$c \oplus k = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0 = m$$

Chiffrement de Vernam: utilisations

- Téléphone rouge (Washington - Moscou)
- Chiffre de Che Guevarra

Problèmes de mise en oeuvre

Principes de Kerkhoffs

1883 Auguste Kerkhoffs, linguiste et cryptographe néerlandais

"La cryptographie militaire": 6 règles pour la cryptographie.

La plus célèbre: la sécurité d'un système cryptographique ne doit dépendre que de la **clé** et non du **secret de l'algorithme** de chiffrement.

Ce principe est systématiquement appliqué aujourd'hui.

Algorithmes standards de chiffrement modernes comme RSA ou AES connus de tous.