CMINF115 — Chapitre 1 : Introduction à la cryptologie. — 10/10/18

I. Définitions.

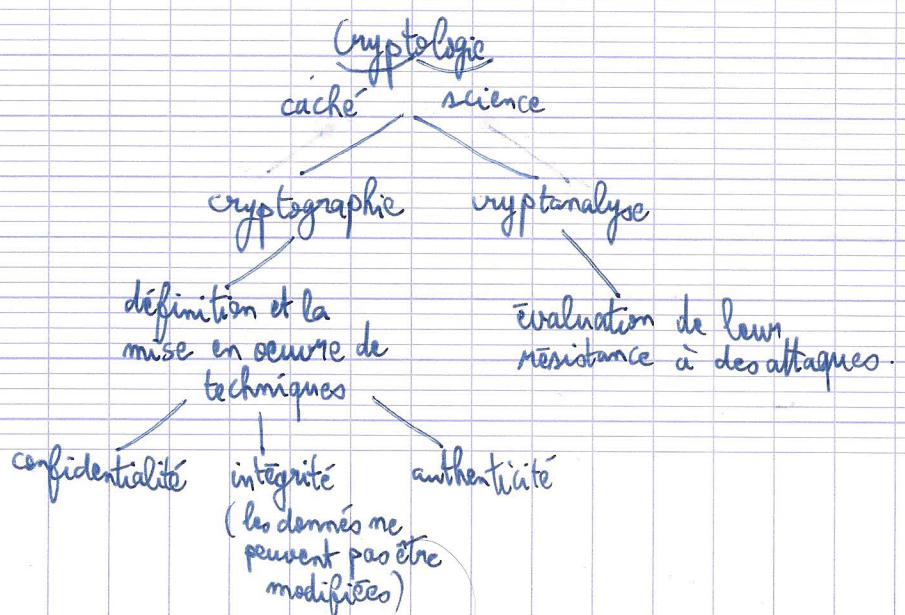
1) Modèle de sécurité en cryptologie :

canal de communication exemple : ondes (GSM, 3G, Wifi)

Idées de sécurisation :
- cable "blindé" : les données circulant dans le canal ne peuvent pas être connues de l'extérieur ; une entité extérieure ne peut pas influencer les données qui circulent ; continuité de la circulation de données ; garantie de qui est l'émetteur des données.
↳ ne marche que pour le filaire ↳ coût élevé ↳ très difficile à réaliser

Définition : La cryptologie est l'ensemble des techniques qui permettent de compenser le fait que le canal de communication n'est pas physiquement sécurisé.

2) Objectifs de sécurité.



3) Notion d'attaquant

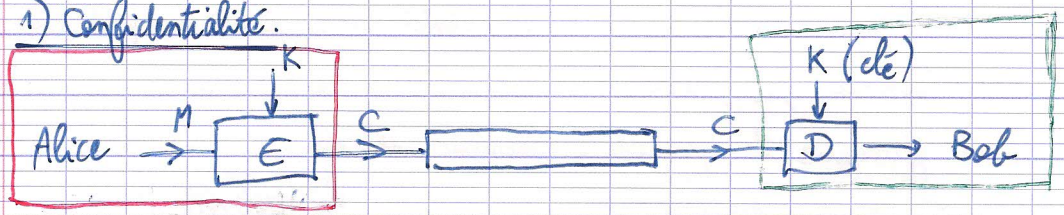
L'attaquant modélise les adversaires et est caractérisé par :
- les informations dont il dispose sur le système
- les moyens dont il dispose.

Et il cherche à mettre en défaut, un (ou plusieurs) des objectifs de sécurité.

Conséquence : on a besoin que (Alice et Bob) connaissent qqch (secret, clé) que l'attaquant ne connaît pas.

II. Le modèle symétrique.

1) Confidentialité.



M : message en clair
C : message chiffré
D : fonction de déchiffrement
E : fonction de chiffrement

$C = E_k(M)$
$M = D_K(C)$
$\forall k, M \quad D_k(E_k(M)) = M$
$\forall K, \boxed{D_K \circ E_K = Id}$

Remarques : K sont inconnus
E et D sont connus par l'attaquant

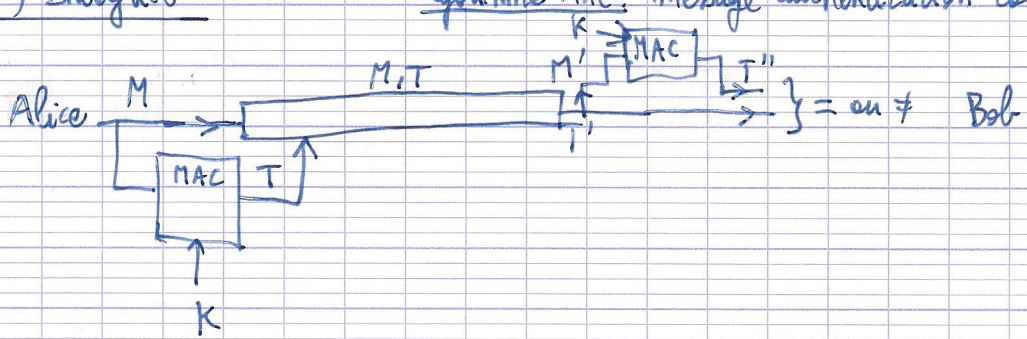
Principe de Kerckhoffs :

La machine de chiffrement doit pouvoir tomber aux mains de l'ennemi sans créer de catastrophe.

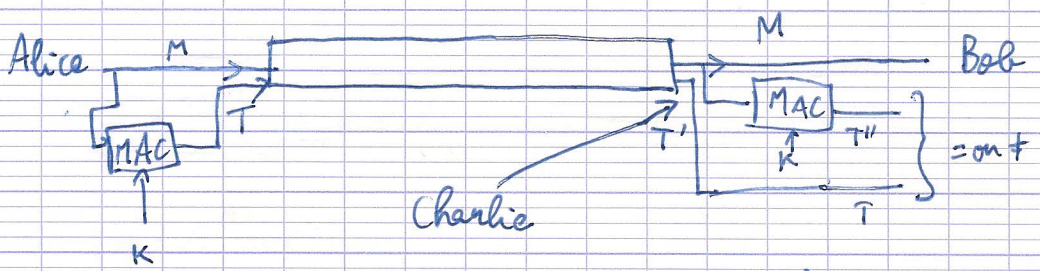
↳ on rend publics les algorithmes cryptographiques.

2) Intégrité

Algorithme MAC : message authentication code



3) Authenticité



Un attaquant Charlie (qui n'est ni Alice ni Bob) ne peut pas se faire passer pour Alice (car il ne connaît pas K)

M : " Moi Alice je donne 50 000 € "

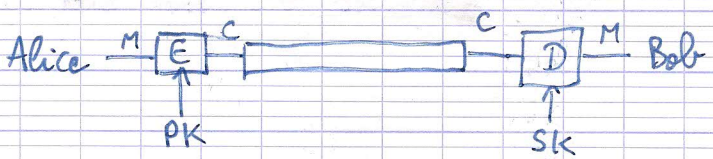
→ problème : Bob peut alors créé lui-même M et $T = MAC_K(M)$.

Conclusion : L'authenticité est impossible dans le modèle symétrique.

III. Le modèle asymétrique.

1) Confidentialité.

1976 : Diffie Hellman "New Directions in Cryptography".

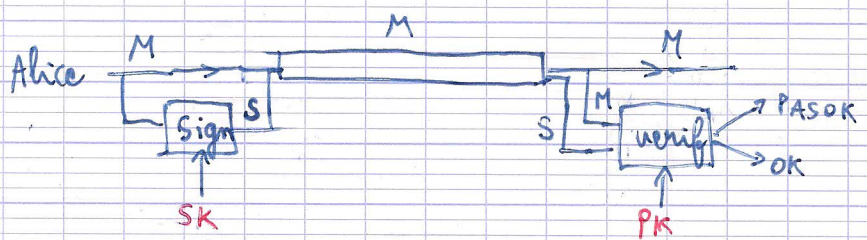


SK : clé secrète
PK : clé publique

$M = D_{SK}(C)$ et $C = E_{PK}(M)$ et $M = D_{SK}(E_{PK}(M))$

$D_{SK} \circ E_{PK} = Id$

2) Integrité et authenticité



$S = Sign_{SK}(M)$

si $S = Sign_{SK}(M) \rightarrow verif_{PK}(M, S) = OK$

	Confidentialité	Integrité	Authenticité
Modèle symétrique	AS DES AES chiffrement symétrique Vigenere	MAC	
Modèle asymétrique	chiffrement asymétrique RSA Elgamal	signature électronique RSA Elgamal	