## Légende

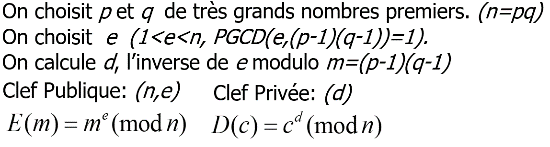
H : Hacker – M : Message – MC : Message chiffré – MD : Message déchiffré – C : Chiffrer ou Encrypter – CM : Chiffrer le/un message – D : Déchiffrer ou décrypter – DM : Déchiffrer le/un message – Bits : Chaîne de bits – MAC : M Authentification Code – PK : Public key – SK : Secret key – RF : Réseau de Fiestel

*AVs* : Avantages – *DAVs* : Désavantages – Mots surlignés : Données manquantes.

Histoire

## Techniques de cryptographie

Stéganographie : Dissimuler des M à l’aide d’un intermédiant – Chiffrement de César : Rotation de l’alphabet (décalage) – Substitution : Remplacer des mots/lettres par un ou plusieurs symboles – Enigma : [Youtube](https://www.youtube.com/watch?v=ASfAPOiq_eQ) . – Data Encryptions Standard (DES): clé de 52 bits; [Youtube](https://www.youtube.com/watch?v=Sy0sXa73PZA) ;RF de 16 rounds – Advanced Encryption Standard (AES) : Consomme peu de mémoire et est très efficace – RSA : [Youtube](https://www.youtube.com/watch?v=-i2WEJiETwY)

  
Difficile, car il faut factoriser de grands nombres.

Introduction

## Les grandes lignes

Confidentialité : Techniques cryptographiques– Conformité : Assurer l’origine et l’intégrité d’un M (authentification, signature électronique) – Accessibilité : Techniques physique (mot de passe, biométrie)

## Établir la sécurité

Politique de sécurité : Claire, complète et précise – Modèle d’adversaire : Un non-médecin ayant accès à un terminal, une panne d’électricité, etc. – Mécanisme de sécurité.

Pour prouver la sécurité d’un système, nous devons avoir un modèle mathématique nous permettant de prouver des théorèmes pour établir que le système n’atteint jamais un état vulnérable.

Confidentialité !

## Chiffrement symétrique

Seulement **ssi** le M peut être C et D par la même clé. Pour assurer le bon fonctionnement, il faut : un bon système de chiffrement par bloc, une bonne façon de choisir le vecteur d’initialisation. – Caractérisé par deux fonctions :

; X chiffre le message M avec la clé k.

; Y déchiffre le secret C avec la clé k.

Sans connaître k, C ne révèle pas d’information sur M.

## Attaques

Quatre attaques possibles : (1) le H possède certains M et MC. Il essaie donc de trouver les clés – (2) le H connaît quelques M qui ont été C par la/les même(s) clé(s). Il essaie alors de DM. – (3) L’attaque à texte clair choisi – (4) L’attaque à texte chiffré choisi.

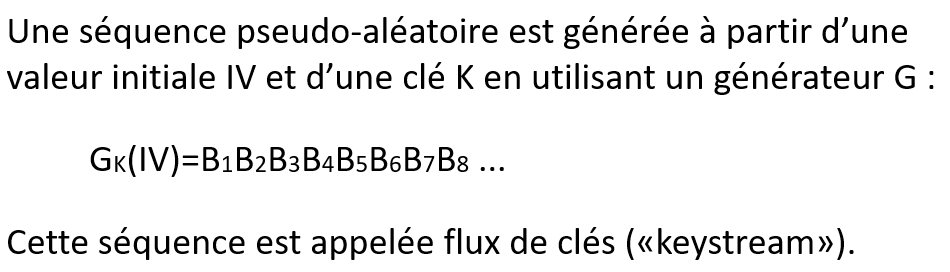
\* Recherche exhaustive de clés.

## Masque Jetable

CM M (CB) à l’aide de la clé k (CB de même longueur ou plus) – Encodage : M XOR clé.

## Chiffre de flux (streamcipher)

Méthode de chiffrement asynchrone spécifiquement conçues pour C un flux de données continu.

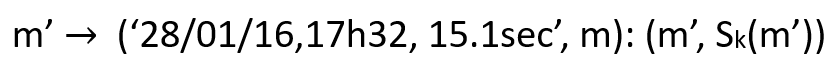
  
Encodage : Comme le Masque jetable, sauf qu’on a

RC4 : Streamcipher le plus connu. Très rapide – Faiblesse : Il faut éviter que la même séquence aléatoire soit générée – Solution : Clé2 = (Clé­1, IV).

Intégrité à partir de clé secrètes

## MAC (MAC)

Permet de valider qu’un M provient bien de notre ami(e) et que celui-ci n’est pas une retransmission envoyée par un H.

S et V sont des algorithmes. – Intégrité != fraîcheur : Pour éviter que H ne retransmette un M déjà reçu, une solution simple est d’ajouter la date au M.   


## Hachage cryptographique

Pour générer des clés, de longueur constante, sans qu’elles ne dépendent du nombre de M à encoder. Fonctions de hachage : MD5, SHA. – Important : Il faut utiliser des clés d’au moins 128bits, car il est possible (paradoxe de l’anniversaire) de trouver une collision dans un temps raisonnable.

## CBC-MAC

N’a pas besoin d’une multitude de sous-clés. Procédure : sépare le M en plusieurs blocs de taille égale (les deux machines s’entendent sur la taille d’un bloc), ajout de « 0 » pour compléter (padding) le dernier bloc, ajoute un bloc au début du M indiquant la taille d’un bloc, utilise le premier bloc du M pour encoder le suivant et ainsi de suite.

Système à clé publique

## Approche

La machine A produit une PK (ou en d’autres mots : le lock) et l’envoie à la machine B (celle qui souhaite communiquer avec A) – La machine B C le contenu du M à envoyer avec la PK reçue – La machine B transmet le MC à la machine A. La machine A D le MC à l’aide d’une SK.

La machine A produit la PK et la SK en même temps. La SK est la seule clé qui peut D des MC par la PK.

Vulnérabilité : fouille exhaustive et autres techniques plus efficaces. Solution : des clés plus longues.

## RSA

RSA est né à cause du problème de la génération de clés secrètes. Le chiffrement du même M produit toujours le même cryptogramme. Il est donc possible de D un MC en ayant en sa possession plusieurs petits MC (dont on connait le MD).

Principes modernes de sécurité : En supposant que le problème Y ne peut être résolu en temps raisonna-ble, le système X est sûr.

Quelle taille de clé pour RSA? Plus le temps avance, plus les ordinateurs sont puissants et peuvent effectuer des calculs plus rapidement. Il faudra augmenter la taille des clés avec le temps.

La sécurité? Nous pouvons choisir e petit (e=3), le niveau de sécurité ne devrait pas être trop affecté – Par contre, d doit être suffisamment grand!!

Efficacité? Les systèmes de C et de D utilisant des clés public (ex : RSA) sont moins efficace que ceux utilisant des clés secrètes. Par contre, ils sont plus versatiles – Il est possible de combiner des techniques pour obtenir le meilleur des deux mondes : partager la clé secrète à l’aide de RSA.

## Signatures

Est-ce que les signatures numériques peuvent avoir la même valeur que les signatures manuscrites? Oui. Problème : Une clé peut être compromise, donc il faut pouvoir invalider les documents signés avec celle-ci. Solution : Utilisation de timestamp pour identifier les transaction (signature + document), comme ça on peut annuler que les transactions concernées. Solution 2 : Faire signer un papier (comme pour les cartes de crédits).

L’intégrité d’une session complète doit être attestée pour conclure qu’elle est sûre. L’intégrité des M n’est pas une solution suffisante.

## Protocole de Diffie-Hellman

Échanger des clés secrètes (clés symétriques) grâce à des méthodes asymétriques (RSA). Utilisé par SSH.