



# Cryptographie

Outils de la cryptographie





# Votre instructeur

Thierry DECKER  
mail@thierry-decker.com

# Cryptographie Outils

Sommaire

- Chiffrement symétrique
  - DES
  - 3DES
  - AES
  - RC4
  - Blowfish
  - Twofish
- Chiffrement asymétrique
  - Diffie-Hellman
  - RSA
  - ECC

# Cryptographie Outils

Sommaire

- Hachage cryptographique
  - SHA
  - MD5
  - RIPEMD
  - HMAC
- Cryptographie de transport
  - SSL/TLS et HTTPS
  - SSH
  - IPSec

# Cryptographie Outils

Sommaire

- Chiffrement Wireless
  - WEP vs. WPA/WPA2
  - Authentification Wi-Fi
- Autre outils de chiffrement
  - PGP/GPG
  - One-time pads
  - CHAP et PAP
  - Chiffrement complet de disque

# Cryptographie Outils

Sommaire

- Forces comparées des algorithmes de cryptographie
  - Algorithmes de confidentialité des données
  - Algorithmes d'intégrité des données



# Chiffrements symétriques

Cryptographie

# Cryptographie Outils DES

- Data Encryption Standard (DES), utilisé pour la confidentialité des données
- Fonctionnement :
  - La clé principale (64 bits) est divisée en 16 sous-clés
  - Les données sont traitées par blocs de 64 bits
  - 16 itérations sur chaque bloc (cycle Feistel)
  - Utilisation d'une sous-clé différente à chaque itération
  - Chaque itération se termine par une phase de substitution et une phase de permutation
- Un des plus anciens algorithmes de chiffrement (choisi en 1979 comme standard par la NSA)
- Vulnérable par rapport aux standards actuels
- Cassable en une journée (à ce jour)



# Cryptographie Outils <sup>3DES</sup>

- Triple Data Encryption Standard
- Utilisé pour la confidentialité des données
- Clé de 168 bits, blocs de 64 bits
- L'algorithme utilise trois passes de "DES" sur chaque bloc
- Chaque passe utilise trois différentes clés dérivées de la clé principale
- Trois fois plus lent que "DES"
- Créé pour augmenter la robustesse de "DES"
- Toujours utilisé à ce jour

# Cryptographie Outils RC4

- Rivest Cipher 4
- Clé dont la longueur est comprise entre 40 et 204 bits
- Utilisé pour la confidentialité en SSL ou WEP
- Chiffrement de flux (pas par bloc)
- Un bit traité à la fois avec un changement de clé pour chaque bit traité
- Développé en 1987 par Ron Rivest
- Ron Rivest a à son actif d'autres algorithmes de chiffrement symétriques (RC1-RC6)
- RC4 a été longtemps le plus utilisé des algorithmes de chiffrement de flux
- Sa robustesse dépend de l'implémentation

# Cryptographie Outils AES

- Advanced Encryption Standard
- Taille de bloc de 128 bits
- Clé de longueur 128, 192 ou 256 bits
- Utilisé pour la confidentialité des données
- WPA2
- Peut être utilisé dans des implémentations à faible utilisation des ressources
- Fonctionnement :
  - Blocs de 128 bits cassés en quatre parties
  - Passes itératives (à la place de passes de Feistel comme dans DES)
  - Nombre de passes dépendant de la longueur de la clé

# Cryptographie Outils AES

- Créé par Rijndael (Rijmen & Daemen) en 2002 et devient le standard américain en remplacement de DES
- Considérer comme sûr à ce jour

# Cryptographie Outils

## Blowfish

- Multi-usage
- Chiffrement par bloc rapide
- Utilise 16 passes Feistel
- Très complexe utilisation des clés
- Produit par Bruce Schneier
- Non breveté depuis sa création
- Considéré comme “fort” s’il est bien implémenté
- Si moins de 16 passes Feistel sont utilisées, il est vulnérable aux attaques
- Taille de bloc de 64 bits
- Clé de longueur 1 à 448 bits

# Cryptographie Outils Twofish

- Cousin de Blowfish et open source
- Multi-usage
- Chiffrement par bloc rapide
- Utilise 16 passes Feistel
- Très complexe utilisation des clés
- Bloc de longueur 128 bits
- Clé de longueur 128 à 256 bits
- Optimisé pour les processeurs 32 bits
- Également créé par Bruce Schneier avec l'aide d'autres cryptographes
- Concurrent direct de AES pour devenir le standard américain
- Considéré comme “fort” s’il est bien implémenté
- Si moins de 16 passes Feistel sont utilisées, il est vulnérable aux attaques



# Chiffrements asymétriques

Cryptographie

# Cryptographie Outils

## Chiffrements asymétrique

- Pas de problème de distribution des clés (publiques -> PKI)
- Moins performants et demandant plus de ressource de traitement



# Cryptographie Outils

## Diffie-Hellman (DH)

- Des noms de Whitfield Diffie et Martin Hellman
- Utilisé :
  - dans le processus d'échange de clés
    - Permet à deux (ou plus) participants qui ne connaissent pas d'échanger une clé secrète partagée
  - Simple à calculer mais extrêmement difficile à inverser
- A la base du concept de paire de clés publique/privée
- Pas d'authentification intrinsèque
- Les clés n'ont pas besoin d'être associées à un utilisateur ou une organisation
- Donc sujet aux attaques de "l'homme du milieu"
- Longueur de clé variable (768, 1024 ou 2048 bits)

# Cryptographie Outils

## Diffie-Hellman

- Alice et Bob veulent utiliser une clé secrète pour chiffrer symétriquement leurs échanges
- S'ils échangent cette clé, celle-ci pourrait être interceptée (rendant le chiffrement sans intérêt)
- Alice et Bob décident d'une couleur commune réputée "publique" (jaune)
- Alice choisit aléatoirement une couleur (rouge)
- Bob choisit aléatoirement une couleur (Bleu)
- Alice combine ces deux couleurs pour en créer une troisième (Jaune+Rouge=Orange)
- Bob combine ces deux couleurs pour en créer une troisième (Jaune+Bleu=Vert)

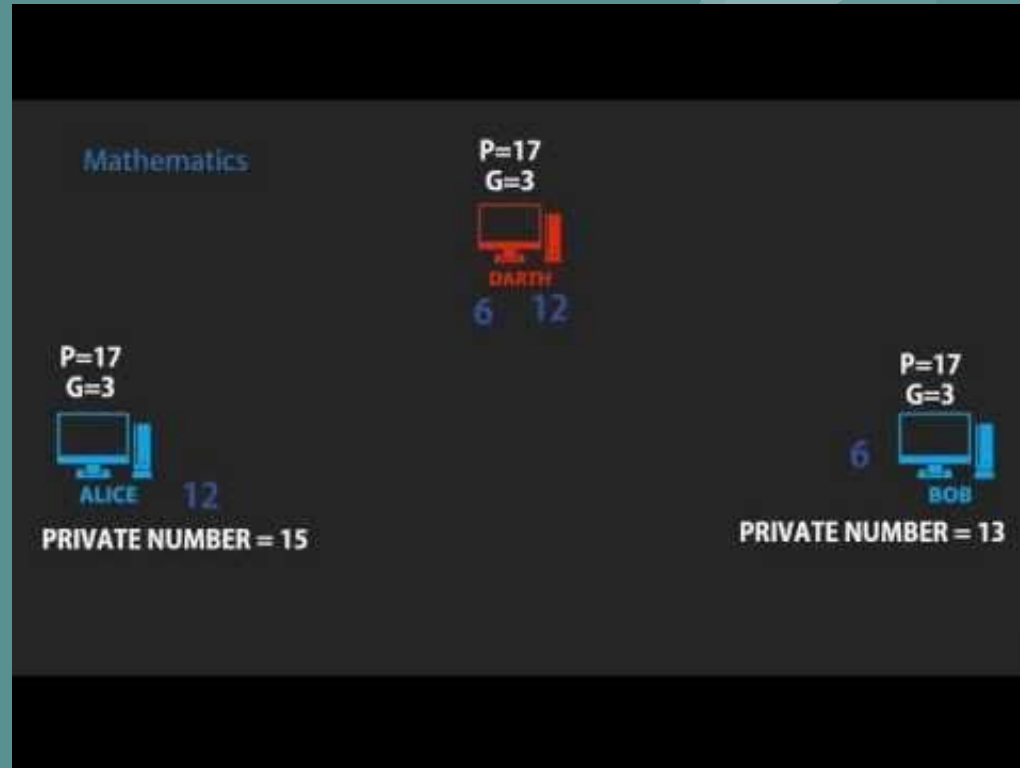
# Cryptographie Outils

## Diffie-Hellman

- Alice envoie sa couleur à Bob (Orange)
- Bob envoie sa couleur à Alice (Vert)
- Alice mélange sa couleur “privée” (Rouge) avec celle envoyée par Bob (vert) : Marron
- Bob mélange sa couleur “privée” (Bleu) avec celle envoyée par Alice (Orange) : Marron
- Un attaquant en possession de toutes les couleurs échangées ne peut créer la couleur “secrète” (Marron) s’il ne possède pas les couleurs secrètes de Alice ET de Bob

# Cryptographie Outils

Diffie-Hellman



# Cryptographie Outils RSA

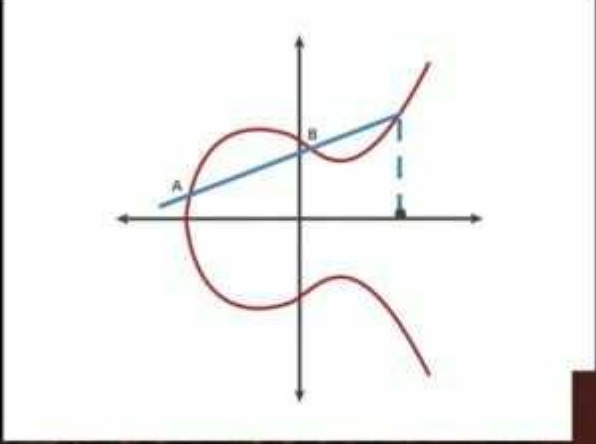
- Un autre algorithme d'échange de clé
- Créé par Ron Rivest, Adi Shamir et Leonard Adleman
- Longueur de clé comprise entre 1024 et 4096 bits
- Confidentialité des données et signature numérique
- Utilise deux très grands nombres premiers (facilité de trouver le produit de deux nombres premiers mais difficulté à trouver deux nombres premiers à partir de leur produit)
- Cent fois plus lent que DES
- Publié à la fin des années 70
- Problème de sécurité si les nombres premiers utilisés sont trop petits

# Cryptographie Outils ECC

- Elliptic Curve Cryptography
- Longueur de clé variable
- Utilisé pour les équipements ayant peu de ressources
- Echange de clé, signature numérique et confidentialité des données
- Une courbe elliptique et un point de cette courbe sont choisis et rendu publics
- Les clés sont calculées depuis cette courbe
- Facilité du calcul mais difficulté de l'inversion
- Beaucoup d'implémentations disponibles
- Beaucoup d'organisations ont leur propre implémentation
- Toujours en phase d'étude mais considéré comme "fort" si les paramètres sont choisis correctement

# Cryptographie Outils

Diffie-Hellman



**FULLSTACK**  
ACADEMY of CODE



# Hachage cryptographique

Cryptographie

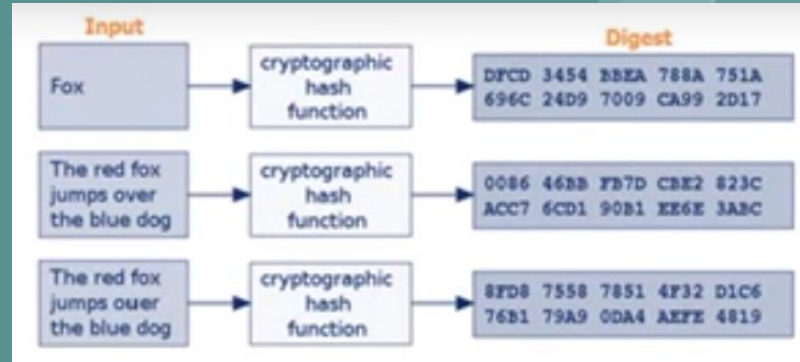


# Cryptographie Outils

## Hachage cryptographique

- Compression des données
- Création d'un "hash" de longueur fixe normalement beaucoup plus court que le message

# Cryptographie Outils Collisions



- Deux messages très peu différents doivent produire un “hash” très différent
- Une collision survient si deux messages différents produisent le même “hash”

# Cryptographie Outils Collisions

- Exemple de collision MD4

## Input A

```
d131dd02c5e6eec4693d9a0698aff95c 2fcab50712467eab4004583eb8fb7f89  
55ad340609f4b30283e4888325f1415a 085125e8f7cdc99fd91dbd7280373c5b  
d8823e3156348f5bae6dacd436c919c6 dd53e23487da03fd02396306d248cda0  
e99f33420f577ee8ce54b67080280d1e c69821bcb6a8839396f965ab6ff72a70
```

## Input B

```
d131dd02c5e6eec4693d9a0698aff95c 2fcab58712467eab4004583eb8fb7f89  
55ad340609f4b30283e488832571415a 085125e8f7cdc99fd91dbdf280373c5b  
d8823e3156348f5bae6dacd436c919c6 dd53e2b487da03fd02396306d248cda0  
e99f33420f577ee8ce54b67080a80d1e c69821bcb6a8839396f9652b6ff72a70
```

## Same Hash Value

```
79054025255fb1a26e4bc422aef54eb4
```

# Cryptographie Outils

## Hachage cryptographique

- Il existe deux risques dégradant la “force” d’un algorithme de hachage
  - L’existence de collisions
  - La possibilité de dé-hacher le “hash” et de retrouver le texte clair à partir du texte chiffré
- Par exemple, on pourrait créer deux documents possédant le même “hash”, faire signer un des documents par la signature numérique du signataire et transférer cette signature numérique sur le second document, à l’insu du signataire...
- Certains algorithmes de hachage peuvent être utilisés pendant des années avant de constater des collisions...

# Cryptographie Outils SHA

- Secure Hash Algorithm
- SHA-256 blocs de 512 bits, longueur de hash de 256 bits
- SHA-512 blocs de 1024 bits, longueur de hash de 512 bits
- Utilisé pour la signature numérique
- Casse les messages en mots et groupe les mots en blocs avant de les traiter en 64 ou 80 passes
- SHA-2 est la version courante (famille de quatre fonctions) :
  - SHA-256 et SHA-512
  - SHA-224 et SHA-384 qui sont des versions réduites
- Les versions avec les plus longs “hash” acceptent des entrées plus longues et traitent des blocs plus grands

# Cryptographie Outils SHA

- Conçus et publiés par la NSA et le NIST
- SHA-1 utilisait des hash de 160 bits et a été remplacé par SHA-2
- SHA-3 a choisi l'algorithme "Keccak" en 2012
- Pas destiné, pour le moment, à remplacer SHA-2, qui n'a pas encore été compromise par une attaque significative
- SHA-1 a révélé l'existence de collisions dans ses algorithmes
- SHA-2 doit être privilégié

# Cryptographie Outils MD5

- Message Digest 5
- Blocs de 512 bits et “hash” de longueur 128 bits
- Preuve de l'intégrité
- Un hash (Message Digest) chiffré avec la clé privée permet d'obtenir une signature numérique
- Casse le message en blocs de 512 bits avec un bourrage obligatoire de 64 bits
- Casse ensuite les blocs en morceaux de 32 bits
- Utilise quatre passes de traitement

# Cryptographie Outils MD5

- Développé en 1991
- Membre de la série d'algorithmes MD2, MD4 et MD6
- MD5 un peu plus lent que MD4 mais plus sûr (MD4 a été cassé et ne devrait plus être utilisé)
- MD6 pas retenu lors la compétition de fonctions de hachage du NIST en 2008
- Des collisions sont possibles dans MD5 et il n'est donc pas considéré comme sûr



# Cryptographie Outils RIPEMD

- RACE Integrity Primitives Evaluation Message Digest
- Taille de bloc variable, 160 bits ou 128 bits (pas sûr)
- Utilisé pour les “Message digest”
- Trois passes de traitement avec des tailles de blocs variables
- RIPEMD est basé sur MD4 et RIPEMD-160 est basé sur MD5
- La version 128 bits à présenté des collisions
- Des versions avec des sorties de plus de 160 bits sont utilisées mais elles ne sont pas plus sûres que la version 160 bits

# Cryptographie Outils HMAC

- Hash-based Message Authentication Code
- Utilisé pour les codes d'authentification des messages (Intégrité et authenticité des messages)
- Fonctionne avec une fonction de hachage ET une clé secrète
  - Par exemple, si SHA256 est utilisé, le résultat est référencé sous le nom HMAC-SHA256
- L'ajout de la clé secrète rend HMAC plus fort que la fonction de hachage utilisée seule



# Chiffrements de transport

Cryptographie

# Cryptographie Outils

Chiffrement de transport

- Sécurisation du transport des informations
- Emails, navigateurs, etc.

# Cryptographie Outils

## SSL/TLS et HTTPS

- Secure Sockets Layer/ Transport Layer Security et Hypertext Transfer Protocol Secure
- SSL/TLS permet HTTPS et d'autre applications client/serveur de communiquer de façon sûre au travers d'un réseau non-sûr
- Offre une protection contre l'espionnage, la falsification de messages pendant leur transport
- HTTPS est "HTTP over TLS"
- TLS utilise un "handshake" permettant aux deux participants de s'authentifier mutuellement ou seulement côté serveur et de définir les paramètres de la communication, incluant une clé symétrique

# Cryptographie Outils

## SSL/TLS et HTTPS

- SSL fut créé par Netscape
- TLS améliore le fonctionnement de SSL et le remplace progressivement
- Sûr seulement si les chiffres et les hash négociés entre les participants sont eux même sûrs
- Sujets à l'attaque du milieu si les protocoles négociés ne sont pas considérés comme sûrs

# Cryptographie Outils SSH

- Secure Shell (remplace Telnet)
- Utilisé pour les sessions distantes, les transferts de fichiers (SCP et SFTP), l'établissement de tunnels, le transfert de ports, etc.
- Pas utilisé pour le trafic entre navigateur et serveur Web
- Utilise un "Handshake" pour choisir les paramètres de communication et échanger une clé de chiffrement symétrique
- Aussi sûr que les algorithmes et fonctions de hachage sélectionnées à l'établissement de la session de communication

# Cryptographie Outils IPsec

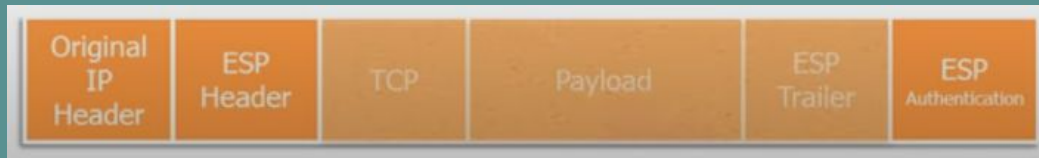
- Internet Protocol Security
- Authentication Header (AH)
  - Signe numériquement les paquets pour leur authentification et leur intégrité
    - Avant un envoie d'un paquet, un hash du paquet et une clé sont calculés
    - Ce hash est ajouté au header et le paquet est transmis
    - Côté récepteur, le payload et la clé secrète sont hachés à nouveau
    - Si le hash d'origine et le nouveau hash concordent, alors nous avons l'authentification et l'intégrité





# Cryptographie Outils IPsec

- Encapsulating Security payload (ESP)
- Ajoute la confidentialité et optionnellement le contrôle d'intégrité
  - Ajoute un header, un trailer et une valeur de contrôle d'intégrité (ICV)
  - Le header ESP inclu des propriétés du paquet comme un numéro de séquence



# Cryptographie Outils IPsec

- Deux modes :
  - Mode transport
    - Seules les données (IP Payload) sont chiffrées et/ou authentifiées
    - le reste du paquet reste inchangé
    - Les adresses IP ne peuvent pas être changées sans corrompre le hash de AH
    - AH ne peut pas être utilisé dans un environnement nécessitant ces modifications d'en-tête
    - Mode utilisé pour les communications d'hôte à hôte

# Cryptographie Outils IPsec

- Deux modes :
  - Mode Tunnel
    - La totalité du paquet est chiffrée et/ou authentifiée
    - Le paquet est ensuite encapsulé dans un nouveau paquet IP avec un nouvel en-tête
    - Supporte donc la traversée de NAT quand le protocole ESP est utilisé
    - Ce mode est utilisé pour créer des réseau privés virtuels (VPN) permettant la communication de réseau à réseau (site-to-site), d'hôte à réseau (accès distant) ou bien d'hôte à hôte (messagerie privée)



# Chiffrement Wireless

Cryptographie

# Cryptographie Outils

## Chiffrement Wireless

- WEP vs WPA vs WPA2

	WEP	WPA	WPA2
Algorithm	RC4	RC4	AES
Key Size	64-bit or 128-bit	128-bit	128 bit
Added Security	None	TKIP	CCMP
Weakness	Can be cracked in a matter of hours	TKIP is vulnerable to spoofing	Denial of Service
Strength	☹	Uses an IV and a second key to produce dynamic per-packet keys	48-bit initialization vector
Integrity Check	Cyclic redundancy check	Message integrity check	
Backward Compatible	N/A	Yes	No

# Cryptographie Outils

## Chiffrement Wireless

- Authentification Wi-Fi
- Pre-shared Key (PSK)
  - Seule solution en WEP
  - WPA-Personal
  - Pour un usage personnel ou les réseaux domestiques
  - Une clé doit être configurée sur les clients et doit correspondre à la clé présente dans le point d'accès
  - Tous les clients partagent une clé
    - WEP : Il est possible de dériver la clé en capturant les paquets
    - WPA : Utilise la clé pour générer des clés dynamiquement
      - La méthode est toujours vulnérable si une pass-phrase faible est choisie comme Pre-Shared Key

# Cryptographie Outils

## Chiffrement Wireless

- Authentification Wi-Fi
- Enterprise Authentication
  - Utilise le protocole 802.1x et un serveur (Radius, ou Diameter ou TACACS+) pour l'authentification



# Autres outils de chiffrement

Cryptographie



# Cryptographie Outils PGP/GPG

- Pretty Good Privacy et GNU Privacy Guard
- Système de chiffrement souvent utilisé avec les Emails
  - Confidentialité des données, authentification et signature numérique
- Les participants doivent tous avoir un client PGP ou GPG
- Utilise aussi bien des algorithmes de chiffrement symétriques que asymétriques
- Crée une “toile” de confiance
  - Un certificat lie une clé à son propriétaire
  - Si vous avez confiance en une personne, vous “signez” son certificat
  - Vous pouvez avoir “confiance” dans les certificats signés par les personnes en lesquelles vous avez confiance

# Cryptographie Outils PGP/GPG

- Pretty Good Privacy et GNU Privacy Guard
- PGP fut introduit en 1991 et disponible commercialement
- GPG a été diffusé en 1999 et n'utilise pas d'algorithme breveté ou à usage restreint par défaut
- La sécurité est bonne selon les implémentations qui en sont faites et tant que la toile de confiance est correctement gérée (signature des certificats)

# Cryptographie Outils OTP

- One-Time Pads
- Utilisé pour la confidentialité des données
- Une clé secrète partagée (pad) de la même longueur que le message
- Cette clé est totalement aléatoire
- Les caractères de la clé sont ajoutés un à un avec ceux du message pour le chiffrer
- L'inverse est fait pour le déchiffrement
- Un concept très ancien décrit vers 1800 et breveté autour de 1900
- Utilisé par l'armée américaine comme outil de cryptographie
- Invulnérable aux attaques en force brute...

# Cryptographie Outils

## CHAP et PAP

- Challenge-Handshake Authentication Protocol
- Password Authentication Protocol
- Authentification sur PPP
- PAP :
  - Utilisateur et mots de passe envoyés en clair pour être vérifiés
  - **NE PLUS UTILISER**
- CHAP :
  - Procédure de réponse au défi pour authentifier le client
  - Le serveur envoie une chaîne de caractère au client
  - Le client hache la chaîne en utilisant une clé secrète partagée et envoie le résultat au serveur
  - Le serveur compare le “hash” envoyé avec celui d’origine

# Cryptographie Outils

Chiffrement complet des disques

- Confidentialité des données stockées
- Protège un disque entier en prévision de vol d'un équipement
- Utilise une clé pour intégralement chiffrer le disque, système d'exploitation compris
- Inclu dans certain systèmes d'exploitation, add-on, dans certaines clés USB , HSM (Hardware Security Module) ou dans certains supports de stockage
- Certains systèmes de chiffrement nécessitent un processeur TPM
- MS Bitlocker et TrueCrypt utilisent AES par défaut avec une clé de 1024 bits
- Si vous perdez la clé, vous perdez les données !
- Certains systèmes possèdent des options de récupération



# Forces comparées des algorithmes de chiffrement

Cryptographie

# Cryptographie Outils

Forces comparées

- Confidentialité des données

Algorithm	Key Length	Mode	Should I Use It?
DES	65-bit	Block	☹
3DES	168-bit	Block	☹
AES	128-bit 192-bit 256-bit	Block	😊😊
RC4	Variable	Stream	☹
Blowfish	64-bit	Block	😊
Twofish	128-bit	Block	😊
One-time Pad	≥ Message Length		☹

# Cryptographie Outils

Forces comparées

- Intégrité des données

Algorithm	Hash Length	Rounds	Should I Use It?
SHA-1	160-bit	80	☹
SHA-2	256-bit or more	64 or 80	☺
MD5	128-bit	4	☹
RIPEMD	128-bit	3	☹
RIPEMD-160	160-bit	3	☺
HMAC	Dependent on hashing algorithm used	Dependent on hashing algorithm used	☺





# Cryptographie Outils - Q&A

Merci de votre attention !