« Long live AES! »

- AES (Advanced Encryption Standard)
  - Nécessité de remplacer DES
  - Concours organisé en 1996 par le National Institute of Standards and Technology (NIST)
  - Cinq algorithmes finalistes internationaux
  - Choix final en 2001
    - Algorithme RIJNDAEL (pron. « *raïndol* »)
      - Proposé par cryptographes belges Joan DAEmen (Proton World Intl.) et Vincent RIJmen (Univ de Louvain)

    - Devient le Advanced Encryption Standard selon les normes :
      - USA - FIPS 197
      - Internationale – ISO/IEC 18033-3

Rijndael (quelques détails)

- Algorithme itératif par bloc
- Plusieurs longueurs de clef et de bloc:
  - 128, (160,) 192, (224,) ou 256 bits (indépendantes l'une de l'autre)
- Une table d'état est utilisée
  - 4 rangées par N_b colonnes avec $N_b = L_{bloc}/32$
- La clef est aussi représentée sous forme de tableau
  - 4 rangées par N_k colonnes avec $N_k = L_{clef}/32$
- Le nombre de cycles (ou « rondes ») de transformation varie de 10 à 14 selon les valeurs de N_b et de N_k
- On procède par une série de transformations/permutations/sélection
  - contrôlées par ces deux tableaux qui sont eux mêmes modifiés à mesure qu'on avance
  - Inspirées d'opérations sur $GF(2^n)$
- Beaucoup plus performant que DES
  - utilisable pour une implantation en matériel.

Rijndael/AES – Avantages et limites

- Principaux avantages
  - performance très élevée
  - possibilité de réalisation sur cartes à puces avec peu de code
  - possibilité de parallélisme
  - pas d'opérations arithmétiques: décalages et XOR seulement
  - n'est pas fondé sur d'obscures relations entres opérations
  - peu de possibilités d'insertion de trappes
  - possibilité de l'utiliser comme fonction de hachage
  - le nombre de rondes peut facilement être augmenté si requis
- Limites
  - le déchiffrement est plus difficile à implanter sur carte à puces
  - code et tables différents pour le chiffrement et le déchiffrement
  - dans une réalisation en matériel, il y a peu de réutilisation des circuits de chiffrement pour effectuer le déchiffrement

Autres normes

- « International Data Encryption Algorithm » (IDEA)
  - proposé comme remplacement de DES
  - chiffre symétrique par bloc
  - blocs de 64 bits, clef de 128 bits

- Les autres finalistes AES
  - Tous: blocks de 128 bits, clés de 128, 192 ou 256 bits
  - Serpent:
    - Anderson, Biham, Knudsen,
  - Twofish/
    - Variante de Blowfish
    - Schneier et al.
  - RC6
    - Variante de RC5
    - Rivest, Robshaw (RSA)
  - Mars

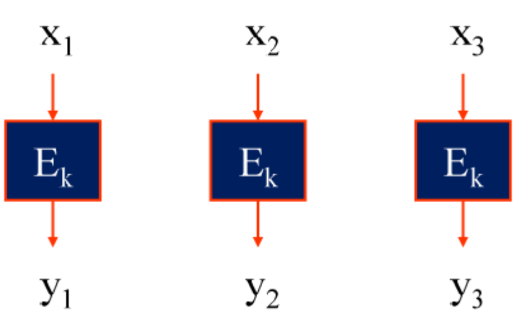
    Don Coppersmith (IBM)

Modes de chiffrement

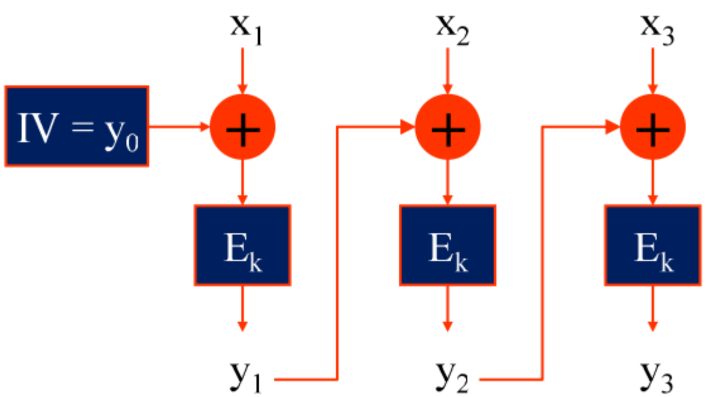
- 4 modes de chiffrement
  - Historiquement introduit suite à la norme DES en 1981 (FIPS 81)
  - Définissent comment appliquer un algorithme de chiffrement par bloc pour la confidentialité de message de taille arbitraire
  - S'applique à n'importe quel algorithme de chiffrement symétrique
- À choisir selon critères d'application
  - Synchrone vs. asynchrone
  - Possibilité d'attaque par texte clair choisi, etc.

Modes de chiffrement

- Electronic Code Book (ECB)
  - Mode traditionnel
  - Chaque bloc chiffré indépendamment
  - La même clé est réutilisée
  - Permet transmission asynchrone

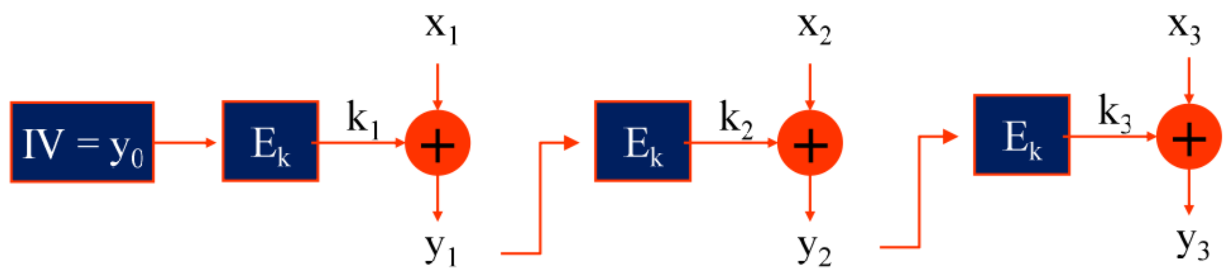


- Cipher Block Chaining Mode (CBC)
  - Chaque bloc XOR-é avec cryptogramme antérieur
  - Utilise un vecteur d'initialisation (IV) comme paramètre cryptographique (pas nécessairement secret)

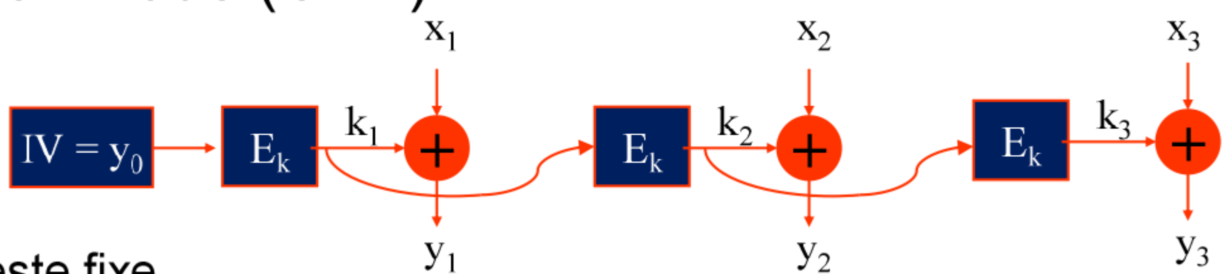


Modes de chiffrement (suite)

- Cipher Feedback Mode (CFB)



  - Clé pour DES reste fixe
  - Clé pour XOR
    - cryptogramme antérieur chiffré par DES
- Output Feedback Mode (OFB)



  - Clé pour DES reste fixe
  - Clé pour XOR
    - Obtenue par application itérative de DES sur IV
    - Peuvent être générées d'avance (indépendante du message)

L'algorithme RC4

- Caractéristiques
  - algorithme cryptographique par flux ("stream cipher")
  - inventé par Ron Rivest
  - secret commercial de RSA Data Security Inc.
  - dévoilé illégalement dans les mi-90
  - utilisé entre autres dans SSL (commerce électronique) et WEP
  - taille de clef variant de 8 à 2048 bits par intervalle de 8
  - génère une séquence pseudo aléatoire de bits
    - Utilisée comme « clé » pour le masque jetable (XORés avec le texte en clair)
  - le déchiffrement consiste à régénérer la séquence de bits et à inverser l'opération XOR
- Fiabilité
  - plusieurs faiblesses ont été identifiées
  - susceptible à une attaque par force brute si
    - la clef est choisie trop courte
    - le clés ou le IV sont mal choisi (basse entropie ou entropie nulle…)

ALGORITHMES À CLÉ PUBLIQUE

POLYTECHNIQUE
MONTRÉAL

UNIVERSITÉ
D'INGÉNIERIE

Notion de groupe

- Notion de groupe $(G, \otimes)$
  - Un ensemble abstrait G sur lequel on a défini une opération abstraite « $\otimes$ » avec certaines propriétés
    - élément identité : $\exists\ 1 \in G$, t.q. $\forall a \in G$, $a \otimes 1 = a$
    - Associativité : $\forall a, b, c \in G$, $a \otimes (b \otimes c) = (a \otimes b) \otimes c$,
    - Tout éléments à un inverse : $\forall a \in G$, $\exists\ a^{-1}$ t.q. $a \otimes a^{-1} = 1$
    - (Commutativité): $\forall a, b \in G$, $a \otimes b = b \otimes a$

      on dit alors que le groupe est "abélien" ou "commutatif"
  - Exponentiation
    - $a^n = a \otimes a \otimes \ldots \otimes a$, n fois

      où n est un entier et $(G, \otimes)$ est un groupe abélien
  - Sous-groupe
    - Un sous-ensemble H de G est un sous-groupe de G si $\forall a$, $a^{-1} \in H$
    - Exemple : Sous-groupe *cyclique*
      - $<a> := \{a^0, a^1, a^2 \ldots\}$ est le sous-groupe cyclique de $(G, \otimes)$ « généré » par a

Calcul en arithmétique modulaire

- S'applique aux nombres entiers non-négatifs seulement
- a modulo b est le reste entier de la division de a par b
- Deux entiers sont équivalents modulo n si leurs modules sont égaux,

$$x \equiv_n y \text{ si et seulement si } (x \bmod n) = (y \bmod n)$$

- Propriétés
  - Associativité: (a + (b + c)) mod n = ((a + b) + c) mod n
    (a * (b * c)) mod n = ((a * b) * c) mod n
  - Commutativité: (a + b) mod n = (b + a) mod n
    (a * b) mod n = (b * a) mod n
  - Distributivité: (a * (b + c)) mod n = ((a * b) + (a * c)) mod n
  - Existence d'identités: (a + 0)mod n = (0 + a) mod n = a
    (a *1) mod n = (1 * a) mod n = a
  - Existence d'inverses: (a + -a) mod n =0
    (a *a^{-1}) mod n = 1 si pgcd(a,n)=1

Arithmétique modulaire
Inverses multiplicatifs

- L'inverse multiplicatif de *a* est *b* tel que $a * b = 1$
  - exemples: (2 * 3) mod 5 => 1; (4 * 4) mod 5 =>1
- Pour un nombre premier *p*
  - (Petit) Théorème de Fermat :
    - a^{p} mod $p = a$,   donc a^{p-1} mod p =1

    2^3 mod 3 = 8 mod 3 = 2;

    4^5 mod 5 = 1024 mod 5 = 4; 4^4 mod 5 = 256 mod 5 = 1;
  - si *x* est l'inverse de *a*
    - $(a * x)$ mod $p = 1 = a^{p-1}$ mod p , donc $x = a^{p-2}$ mod p (p premier)
- En général, pour un entier *N*
  - Théorème d'Euler :
    - $a^{\varphi(N)} = 1$ mod N
  - MAIS, l'inverse de *a* existe seulement si pgcd $(a,N) = 1$

Groupes pertinents

- Ensembles en arithmétique modulaire
  - $Z_N = \{a \in Z : 0 < a < N\}$
  - $Z_p^* = Z_p - \{0\} = \{a \in Z : 0 < a < p\}$, ou p est premier
  - $Z_N^* = \{a \in Z : 0 < a < N, \text{pgcd}(a,N) = 1\}$

- Groupes pertinents
  - $(Z_N, +)$ est un groupe commutatif
    - Tout $a \in Z_N$ a un inverse additif $-a$
  - $(Z_N, *)$ n'est pas un groupe
    - Si pgcd $(a,N) = d > 1$, alors $a*d = 0$
      - a,d sont des diviseurs de 0
      - a n'a pas d'inverse multiplicatif a^{-1} t.q. $a^{-1} a = 1$
  - $(Z_N^*, *)$ et $(Z_p^*, *)$ sont tous les deux des groupes commutatifs

Groupe multiplicatif Z_N^*

- Combien d'éléments dans Z_N^*?
  La fonction d'Euler $\varphi(n)$ donne la réponse
  - si p est premier:
    - $\varphi(p) = p - 1$
    - $\varphi(p^k) = p^{k-1} (p - 1)$
  - si p,q sont relativement premier
    - $\varphi(p*q) = \varphi(p)\, \varphi(q)$
  - en particulier si $N = p * q$, avec p et q premiers
    - $\varphi(N) = \varphi(p) * \varphi(q) = (p - 1) * (q - 1)$

- Quelle est la structure de Z_N^* ?
  - Tous les sous-groupes sont isomorphes à $\langle a \rangle$ pour un a dans Z_N^*
  - Les tailles (ou ordre) de ces sous-groupes sont les facteurs de $\varphi(N)$

Exemples de Z_N^*

- $N = 12 = 2^2 * 3$
  - $Z_{12}^* = \{1, 5, 7, 11\}$
  - $\varphi(12) = \varphi(2^2)\ \varphi(3) = 2 * 2 = 4$
    - Le seul diviseur de $\varphi(12)$ est 2

    ➔ Tous les éléments ont un ordre 2 ou 4
  - En effet
    - $5^2 = 25 = 1 \Rightarrow \langle 5 \rangle = \{1,5\}$
    - $7^2 = 49 = 1 \Rightarrow \langle 7 \rangle = \{1,7\}$
    - $11^2 = 121 = 1 \Rightarrow \langle 11 \rangle = \{1,11\}$
  - Noter qu'aucun élément à ordre 4

- $N = 15 = 3*5$
  - $Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$
  - $\varphi(15) = \varphi(3)\ \varphi(5) = 2 * 4 = 8$
    - Les seuls diviseur de $\varphi(15)$ sont 2 et 4 ➔ Tous les éléments ont un ordre 2, 4 ou 8
  - En effet
    - $2^1 = \underline{2},\ 2^2 = \underline{4},\ 2^3 = \underline{8},\ 2^4 = \underline{1}$
      - $\Rightarrow \langle 2 \rangle = \{1,2,4,8\}$
      - $\Rightarrow \langle 4 \rangle = \{1,4\}$
      - $\Rightarrow \langle 8 \rangle = \{1,8,4,2\}$
    - $7^2 = 4,\ 7^3 = 28 = 13,\ 7^4 = 91 = 1$
      - $\Rightarrow \langle 7 \rangle = \{1,7,13,1\}$
    - $11^2 = 121 = 1$
      - $\Rightarrow \langle 11 \rangle = \{1,11\}$
    - $13^2 = 4,\ 13^3 = 52 = 7,\ 13^4 = 91 = 1$
      - $\Rightarrow \langle 13 \rangle = \{1,4,7,1\}$
    - $14^2 = (-1)^2 = 1$
      - $\Rightarrow \langle 14 \rangle = \{1,14\}$
  - Noter qu'aucun élément à ordre 8

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

INF 4420: Sécurité Informatique
Cryptographie II

INF4420: Éléments de Sécurité Informatique
Identification, Authentification

Nora Cuppens

Contenu du cours

- Authentification et gestion des identités
- Authentification par mot de passe
- Gestion des mots de passe
- Authentification deux facteurs
- Authentification mutuelle

Gestion des identités et des accès

- Authentification
  - « Est-ce que c'est la bonne personne/système ? »
  - Identification usager ➔ système
  - Identification système ➔ système
  - Identification système ➔ usager
- Autorisation
  - « Est-ce que cette personne a le droit de faire ça ? »
  - Contrôle d'accès
    - Physique vs. logique
    - Objet protégés et modes d'accès
    - Modèles de contrôle d'accès

Authentification des usagers

- Les 4 modes d'authentification d'un usager

- Par quelque chose qu'il connaît
- Par quelque chose qu'il est (biométrie statique)
- Par quelque chose qu'il possède
- Par quelque chose qu'il fait (biométrie dynamique)