INF4420a: Sécurité Informatique

Cours 4 : Exercices Crypto

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Exercice 1 : Sécurité de DES et 3DES

- Objectif :
  - Comprendre pourquoi en chiffrant plusieurs fois, avec des clés différentes, on ne rallonge pas forcément la longueur de la clé
  - Comprendre pourquoi 3DES reste aujourd'hui difficile à casser

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Exercice 1 : Sécurité de DES et 3DES

- Rappel de cours
  - DES = chiffrement symétrique (ou à clé secrète)
  - Clé de chiffrement = clé de déchiffrement
  - DES repose sur une clé de chiffrement de 64 bits
  - Mais en fait la clé correspond à 56 bits « utiles »
  - Les 8 derniers bits servent pour le contrôle de parité

  - DES est désormais considéré obsolète

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Question 1 : Si on applique DES 2 fois avec la même clé de chiffrement, le résultat obtenu va être équivalent à un chiffrement avec une clé de :
  - 56 bits ?
  - 57 bits ?
  - 112 bits ?

$$m \xrightarrow[k_1]{} E(k_1,m) \xrightarrow[k_1]{} E(k_1, E(k_1,m))$$

Exercice de crypto

- Réponse question 1 : 56 bits
- Explication : Cassage de DES par force brute

$$E(k_1,m) \xrightarrow[k\ ?]{} D(k, E(k_1,m)) = m \text{ si } k = k_1$$

  - Clés de N bits= 2^N clés possibles
  - Plus facile de reconnaître m si l'attaquant connait des correspondances (m, $E(k_1,m)$)
    - **Attaque à texte clair connu**

Exercice de crypto

- Réponse question 1 (suite) : Cassage de $E(k_1, E(k_1,m))$ par force brute

$$M=E(k_1,E(k_1,m)) \xrightarrow[k\ ?]{} D(k, M) \xrightarrow[k\ ?]{} D(k,D(k,M))$$

- On a $D(k,D(k,M)) = m$ si $k = k_1$
- On doit toujours tester 2^N cas possibles pour une clé de N bits
  - C'est juste un peu plus long pour déchiffrer

Exercice de crypto

- Question 2 : Si on applique DES 2 fois avec des clés de chiffrement différentes, le résultat obtenu va être équivalent à un chiffrement avec une clé de :
  - 56 bits ?
  - 57 bits ?
  - 112 bits ?

$$m \xrightarrow[k_1]{} E(k_1,m) \xrightarrow[k_2]{} E(k_2, E(k_1,m))$$

Exercice de crypto

- Réponse question 2 : 57 bits (c'était dans le cours)

- Explication : Analyse de 2DES
  - On applique DES 2 fois avec des clés différentes

$$m \xrightarrow[k_1]{} E(k_1,m) \xrightarrow[k_2]{} E(k_2, E(k_1,m))$$

  - On espère avoir ainsi « doublé » la taille de la clé
  - Soit 56 * 2 = 112 bits
  - Pourquoi ?

Exercice de crypto

- Explication question 2 : Cassage de $e(k_2, e(k_1,m))$ par force brute « naïve »

$$M=E(k_2,E(k_1,m)) \xrightarrow[k\ ?]{} D(k, M) \xrightarrow[k'\ ?]{} D(k',D(k,M))$$

  - **Dans ce cas, on a $D(k',D(k,M)) = m$ si $k = k_1$ ET $k' = k_2$**
  - **Mais on doit tester $2^N * 2^N$ cas possibles soit $2^{N+N} = 2^{2*N}$**
  - **Il semble donc qu'on ait doublé la clé**

– Question : Que peut faire l'attaquant pour faire (beaucoup) mieux ?

  - **Indice 1 : Penser à une attaque à texte clair connu**

Exercice de crypto

- Indice 2 : L'attaque s'appelle « rencontre du milieu »
  - Meet In the Middle Attack en Anglais (MITM)

Exercice de crypto

- Réponse question 2 : L'attaquant réalise une attaque MITM
  - Supposons que l'attaquant connait m et M = $E(k_2,E(k_1,m))$ pour une paire (m, M)
  - Alors l'attaquant peut calculer :

$$m \xrightarrow[k\ ?]{} C = E(k,m)$$

$$M \xrightarrow[k'\ ?]{} C' = D(k',M)$$

  - Si C = C', alors (k, k') est une paire de clés candidates

Exercice de crypto

- Réponse question 2 (suite) : Attaque MITM
  - Les paires de clés candidates sont en général en petit nombre
  - L'attaquant peut ensuite tester les paires de clés candidates sur d'autres messages pour retrouver k_1 et k_2

Exercice de crypto

- Réponse question 2 (suite) : Attaque MITM
  - Bilan de l'attaque

$$m \xrightarrow[k\ ?]{} C = E(k,m) \Rightarrow \mathbf{2^{56}\ cas\ possibles}$$

$$M \xrightarrow[k'\ ?]{} C' = D(k',M) \Rightarrow \mathbf{2^{56}\ cas\ possibles}$$

  - L'attaquant doit donc faire de l'ordre de $2^{56} + 2^{56} = 2^{57}$ calculs
  - Le double DES est donc « équivalent » à un chiffrement avec une clé de 57 bits

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Une MITM est une attaque de type « compromis temps mémoire »

- Pour réaliser une attaque MITM, l'attaquant doit disposer :
  - D'un espace de stockage très grand (hypothèse 1)
  - D'un algorithme de comparaison de chaînes de caractères très rapide (hypothèse 2)

Exercice de crypto

- Question 3 : Quel espace de stockage est nécessaire pour réaliser une attaque MITM dans le cas du 2DES ?
  1. Environ 500 * 10^{12} octets (500 Téraoctets)
  2. Environ 500 * 10^{15} octets (500 Pétaoctets)
  3. Environ 500 * 10^{18} octets (500 Exaoctets)

Exercice de crypto

- Réponse question 3 : Environ $500 * 10^{15}$ octets (500 Pétaoctets)
  - Dans le cas de DES, clés de 56 bits et blocs de 64 bits
  - Espace de stockage nécessaire :
    - $2^{56} * 2^{6} = 2^{62} = 4 * 2^{60} \approx 4 * 10^{18}$ bits
    - $4 * 10^{18}$ bits = $500 * 10^{15}$ octets
  - Il faut donc disposer d'un espace de 500 pétaoctets
    - Soit 500 000 téraoctets
    - Irréalistes à la création de DES
    - Mais tout à fait possible aujourd'hui, voir : http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/

Exercice de crypto

- Question : L'hypothèse 2 (besoin d'un algorithme de comparaison de chaînes de caractères très rapide) est-elle réaliste ?
  - Difficile de répondre
  - Des idées ?

Exercice de crypto

- Analyse de 3DES
  - On utilise toujours deux clefs
  - On réalise trois opérations: $E(k_1, D(k_2, E(k_1, m)))$

- Question 4 : 3DES est équivalent à un chiffrement avec une longueur de clé égale à :
  - 57 bits (= 56 + 1)
  - 112 bits (= 56 * 2)
  - 113 bits (= 56 * 2 + 1)
  - 168 bits (= 56 * 3)

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Réponse question 4 : 112 bits est la bonne réponse !
  - C'était dans le cours…

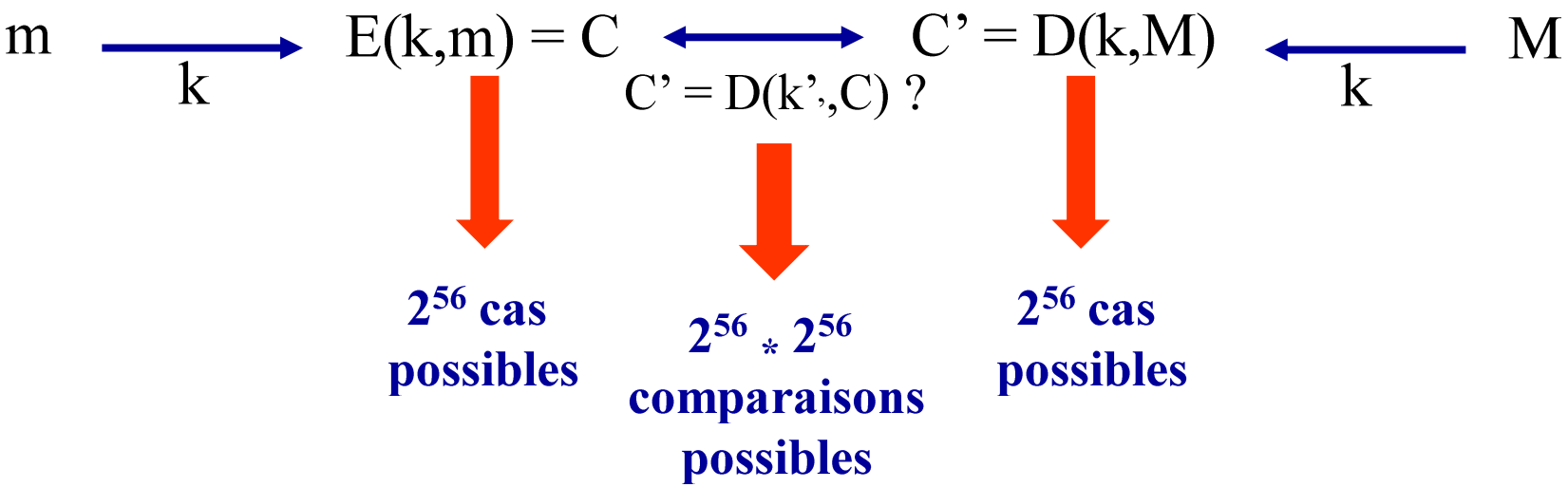
- Pourquoi ?

Exercice de crypto

- Réponse question 4 :
  - Attaque en texte clair connu
  - L'attaquant connait m et M = $E(k_1, D(k_2, E(k_1, m)))$
  - Que peut faire l'attaquant ?
    - Une attaque MITM !
  - L'attaquant calcule E(k,m) pour toutes les clés possibles
    - Il obtient $C = E(k_1,m)$ pour $k = k_1$ mais il ne sait pas où est C
  - L'attaquant calcule D(k,M) pour toutes les clés possibles
    - Il obtient $C' = D(k_2, E(k_1, m))$ pour $k = k_1$ mais il ne sait pas où est C'
  - On a donc $C' = D(k_2,C)$
    - Mais l'attaquant ne sait pas où est C ni où est C'

Exercice de crypto

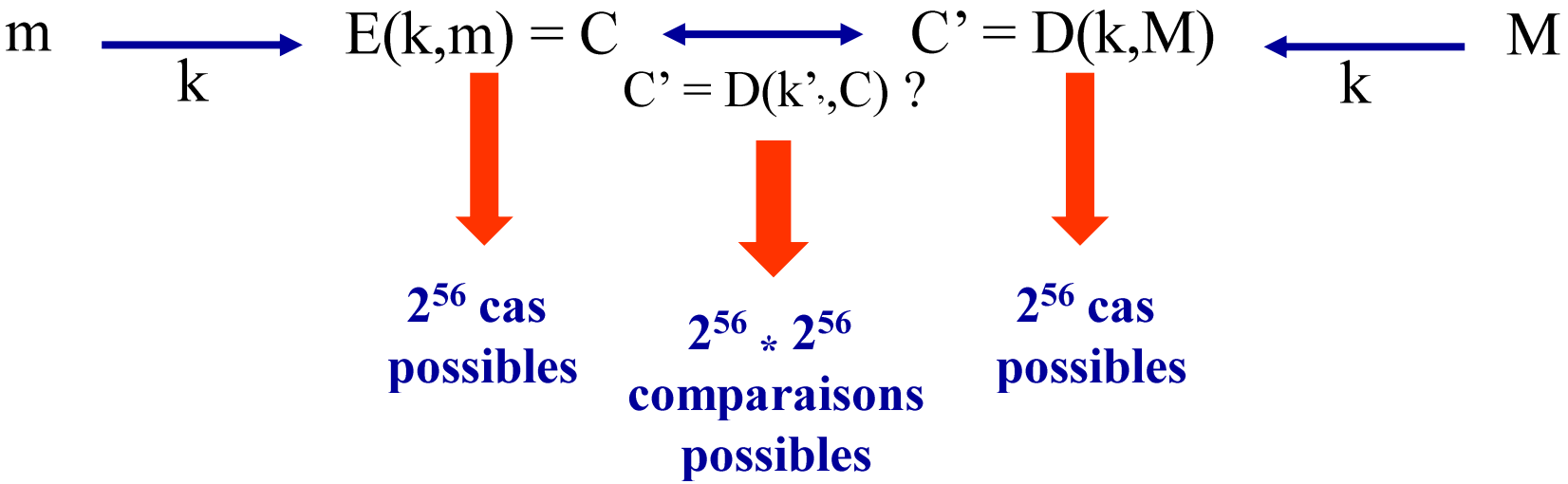
- Réponse question 4 :



- Calculs de l'attaquant (cas pire)
  - $2^{56} + 2^{56} + 2^{56} * 2^{56} \approx 2^{112}$
  - Équivalent à une clé de 112 bits

Exercice de crypto

- Réponse question 4 :



- Calculs de l'attaquant (cas pire)
  - Toujours besoin d'un espace de stockage de 500 pétaoctets !

Exercice de crypto

- Analyse de 3DES
  - On utilise toujours deux clefs
  - On réalise trois opérations: $E(k_1, E(k_2, E(k_1, m)))$
    - On a remplacé un déchiffrement par un chiffrement

- Question 5 : Est-ce que ça change quelque chose ?
  - Oui
  - Non

Exercice de crypto

- Analyse de 3DES
  - On utilise toujours deux clefs
  - On réalise trois opérations: $E(k_1, E(k_2, E(k_1, m)))$
    - On a remplacé un déchiffrement par un chiffrement

- Question 5 : Est-ce que ça change quelque chose ?
  - Oui
  - Non

- Réponse question 5 : Non, ça ne change pas grand chose

Exercice de crypto

- Analyse de 3DES
  - On utilise toujours deux clefs
  - On réalise trois opérations: $E(k_1, E(k_1, E(k_2, m)))$
  - On a changé l'ordre de chiffrement

- Question 6 : Est-ce que ça change quelque chose ?
  - Oui
  - Non

Exercice de crypto

- Analyse de 3DES
  - On utilise toujours deux clefs
  - On réalise trois opérations: $E(k_1, E(k_1, E(k_2, m)))$
  - On a changé l'ordre de chiffrement

- Réponse question 6 : Oui, ça change tout !
  - L'attaquant calcule E(k,m) et D(k',D(k',M))
  - Il compare comme pour 2DES
  - On obtient une clé équivalente à 57 bits !

Exercice de crypto

- 4DES ?
  - On utilise trois clefs
  - On réalise quatre opérations, par exemple :

$$E(k_1, E(k_2, E(k_3, E(k_1,m))))$$

- Question 7 : 4DES serait équivalent à un chiffrement avec une longueur de clé égale à :
  - 112 bits (= 56 * 2)
  - 113 bits (= 56 * 2 + 1)
  - 168 bits (= 56 * 3)

Exercice de crypto

- 4DES ?
  - On utilise trois clefs
  - On réalise quatre opérations, par exemple :

$$E(k_1, E(k_2, E(k_3, E(k_1,m)))) = M$$

- Réponse question 7 : 113 bits
  - L'attaquant calcule D(k, D(k',m)) pour tous les couples de clés (k,k') → 2^{112} cas possibles
  - L'attaquant calcule D(k,D(k',M)) pour tous les couples de clés (k,k') → 2^{112} cas possibles
  - Il compare

Exercice de crypto

- 4DES ?
  - On utilise trois clefs
  - On réalise quatre opérations, par exemple :

$$E(k_1, E(k_2, E(k_3, E(k_1,m)))) = M$$

- Réponse question 7 : 113 bits
  - Au final, l'attaquant a fait de l'ordre de $2^{112} + 2^{112} = 2^{113}$ calculs
  - Il faudrait passer au 5DES pour avoir une clé théorique de 168 bits
  - Par contre, l'attaque MITM n'est plus réaliste car il faudrait un espace mémoire de l'ordre de 2^{112} blocs mémoire, soit 2^{118} bits pour des blocs de 64 bits !

Exercice de crypto

- Exercice 2 : Sécurité de 3DES

- Objectif :
  - Analyser la sécurité de 3DES
  - Autrement dit, est-ce qu'un algorithme de chiffrement symétrique avec une clé de 112 bits, est-il aujourd'hui sécuritaire ?
  - Et a fortiori, un chiffrement symétrique avec une clé de 128 bits comme conseillé pour AES

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Exercice 2 : Sécurité de 3DES
- Rappel de cours
  - 3DES est équivalent à un algorithme avec une clé de 112 bits
  - Un seul COPACABANA permet de tester environ 2^{38} clés par seconde
- Question 1 : Avec un seul COPACABANA, combien de temps faudrait-il pour craquer 3DES par force brute ?
  1. Environ 500 ans
  2. Environ 500 000 ans
  3. Environ 500 milliards d'années
  4. Environ 500 000 milliards d'années

Exercice de crypto

- Exercice 2 : Sécurité de 3DES
- Réponse question 1 : 4. 500 000 milliards d'années !
- Nombre de secondes nécessaires pour casser 3DES avec COPACABANA :
  - $2^{112} / 2^{38} = 2^{74}$ secondes
- Nombre de secondes dans une année :
  - $60 * 60 * 24 * 365 = 31\,536\,000 \approx 32 * 10^6 \approx 2^5 * 2^{20} = 2^{25}$
- Nombre d'années nécessaires pour casser 3DES
  - $2^{74} / 2^{25} = 2^{49} = 2^9 * 2^{40} \approx 500 * 10^{12} \approx$ 500 000 milliards d'années

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Exercice 2 : Sécurité de 3DES

- On suppose un scenario apocalyptique comme dans le film “La Matrice” avec un COPACABANA et un panneau solaire sur chaque mètre carré de la Terre (océan et continent)

Exercice de crypto

- Exercice 2 : Sécurité de 3DES

- Question 2 : Combien de temps faudrait-il « aux machines » pour craquer 3DES par force brute ?
  1. Environ 1 an
  2. Environ 10 ans
  3. Environ 100 ans
  4. Environ 1000 ans

- Indication :
  - La surface de la terre est d'environ 500 millions de km^2

Exercice de crypto

- Exercice 2 : Sécurité de 3DES
- Réponse question 2 : Environ 1 an
- Nombre de COPACABANA sur terre :
  - 500 millions de km^2 = 500 * 10^6 * 10^6 = 500 * 10^{12}
- Nombre d'années nécessaires aux machines pour casser 3DES
  - 500 * 10^{12} / 500 * 10^{12} = 1 an

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Exercice 2 : Sécurité de 3DES

- D'après la loi de Moore, la capacité de calcul d'un ordinateur double tous les 18 mois

- Question 3 : En supposant que COPACABANA va suivre la loi de Moore, dans combien de temps un COPACABANA mettra moins d'un an pour casser 3DES ?
  - Moins de 10 ans
  - Moins de 100 ans
  - Moins de 1000 ans
  - Moins de 10000 ans

Exercice de crypto

- Exercice 2 : Sécurité de 3DES

- Réponse question 3 : 2. Moins de 100 ans

- Aujourd'hui, il faut 2^{49} années pour casser 3DES
- On divise ce temps par 2 tous les 18 mois (soit 1,5 an)
- Nombre d'années nécessaires pour casser 3DES en moins d'un an :
  - 49 * 1,5 = 73,5 années

Exercice de crypto

- Exercice 3 : Sécurité de DES (question 18 de l'examen intra A2014)
- Vous êtes en possession d'une boîte noire qui fait 200 déchiffrements à la seconde. Quel est le temps moyen pour monter une attaque par force brute à l'aide d'un texte connu (vous possédez un exemplaire chiffré et déchiffré du même texte) pour un algorithme ayant une taille effective de clé de 56 bits ?
  a. Approximativement 10 740 000 ans.
  b. Approximativement 14 000 ans.
  c. Approximativement 300 ans.
  d. Approximativement 2 200 ans.
  e. Approximativement 5 370 000 ans.

Exercice de crypto

- Bonne réponse : e. 5 370 000 ans
- Nombre de seconde dans une année :
  - 60 * 60 * 24 * 365 = 31 536 000 ≈ 32* 10^6 ≈ 2^25
- Nombre d'opérations de déchiffrement réalisées par an :
  - 200 * 2^25
- Nombre d'années nécessaires pour casser une clé de 56 bits par force brut (cas pire nécessaire pour tester toutes les clés possibles) :
  - 2^56 / (200 * 2^25) ≈ 10 737 418 ans
- Le temps moyen sera statistiquement égal à la moitié du cas pire :
  - 10 337 418 / 2 = 5 368 709 ans