INF4420a: Sécurité Informatique

Exercices Crypto III

Frédéric Cuppens, José M. Fernandez, Nora Cuppens

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Exercice 1 : Apocalypse mécanique (Question 4 de l'examen d'automne 2010)

- Objectif :
  - Savoir évaluer le temps nécessaire pour casser une clé par force brute
  - Savoir évaluer la taille de la clé en fonction des capacités de calcul de l'adversaire

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Exercice 1 : Apocalypse mécanique (Question 4 de l'examen d'automne 2010)

- Les robots ont pris le contrôle de la planète
- Quelques humains résistent et communiquent avec un ordinateur Mainframe utilisant un chiffrement AES avec clés de 128 bits
- Les robots doivent prendre le contrôle de cet ordinateur avant que le prochain Néo n'arrive sur Terre dans 10000 ans pour organiser la révolte

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Exercice 1 : Apocalypse mécanique (Question 4 de l'examen d'automne 2010)

- Il y a environ 500 milliard de machines sur toute la planète
- Chaque machine est capable de tester environ 1000 billions (billion = 10^{12}) de chiffrement AES par seconde (un chiffrement à chaque nanoseconde)

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Question 1 : Est-ce que les robots réussiront à prendre le contrôle du Mainframe avant le retour de Néo ?
  - Oui
  - Non

Exercice de crypto

- Réponse question 1 :
  - Nombre total de clés AES à tester
    - 2^128 clés
  - 500 milliards de machines
    - 500 * 10^9 ≈ 500 * 2^30 ≈ 2^39 machines
  - 1000 billion clés / s
    - 10^15 clés / s ≈ 2^50 clés par sec
  - Nombre total de clés essayées par seconde
    - 2^50 * 2^39 clés / sec = 2^89 clés
  - Nombre de secondes par année
    - 60*60*24*365 = 31 536 000 ≈ 32 * 10^6 sec ≈ 2^25 sec / année
  - Nombre total de clés essayées par année
    - 2^89 * 2^25 = 2^114 clés / année
  - Temps total pour essayer toutes les clés
    - 2^128 / 2^114 clés = 2^14 année = 16384 années

Exercice de crypto

- Réponse question 1 :
  - Non, les robots ne sont pas sûr de réussir à prendre le contrôle du Mainframe avant le retour de Néo !
  - Mais, ils ont quand même des chances d'y arriver

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Pour éviter l'attaque, les humains changent l'algorithme AES pour l'algorithme à clé publique RSA
- Pour transmettre leur message, les humains utilisent des capcha que les robots ne savent pas reconnaître
- Les robots entrainent des humains pour faire la reconnaissance à leur place
- Les humains entrainés sont connectés à la Matrice et peuvent tester jusqu'à 100 clés par seconde
- Les robots sont capables d'alimenter 100 milliards d'humains

Exercice de crypto

- Question 2 : Quelle est la longueur minimum de clé RSA que les humains devraient choisir pour être protégés jusqu'à l'arrivée du prochain Néo ?
  - Au minimum 45 bits
  - Au minimum 83 bits
  - Au minimum 128 bits
  - Au minimum 145 bits

Exercice de crypto

- Réponse question 2 :
  - Nombre d'humains
    - 100 * 10^9 ≈ 100 * 2^30 ≈ 2^37 humains
  - Nombre de clés / s par humain
    - 100 clés / s ≈ 2^7 clés / s
  - Nombre total de clés testé / s
    - 2^7 * 2^ 37 = 2^44 clés
  - Nombre de secondes avant l'arrivée du prochain Néo
    - 10 000 * 2^25 < 2^14 * 2^25 = 2^39
  - Nombre de clés essayées avant prochain Néo
    - 2^39 * 2^44 = 2^83

Exercice de crypto

- Réponse question 2 :
  - Les robots pourront tester 2^83 clés en 10000 ans
  - Afin d'éviter une « bad luck » (les machines tombent sur la bonne clé rapidement), la clé devrait dont avoir idéalement au minimum 90 bits

Exercice de crypto

- Les robots ont découvert qu'il existait une méthode beaucoup plus rapide de casser RSA que la force brute
- Pour cela, ils ont récupéré une implémentation de l'algorithme de factorisation de Pollard (la méthode de « rho ») qui a un temps d'exécution de $O(2^{n/3})$ opérations, où n est la taille en bits de l'entier à factoriser
- En optimisant cet algorithme, les robots ont réussi à l'exécuter en exactement $1/1000 \cdot 2^{n/3}$ opérations pouvant être réparties sur l'ensemble des machines de la Terre
- Les robots ont aussi réussi à optimiser leurs machines pour que chacune calcule jusqu'à 10^{18} opérations par seconde

Exercice de crypto

- Question 3 : Évaluez l'impact que cette découverte pourrait avoir pour les humains. Quelle devra être la taille minimale de la clé dans ce cas ?
  1. 128 bits
  2. 190 bits
  3. 444 bits
  4. 500 bits

Exercice de crypto

- Réponse question 3 :
  - Nombre de machines
    - 2^39 machines
  - Nombre d'opérations par seconde
    - 10^18 ≈ 2^60 / s
  - Nombre d'opérations par année
    - 2^60 * 2^25 = 2^85 / an
  - Nombre d'opérations avant Néo
    - 2^85 * 2^39 * 10000 < 2^85 * 2^39 * 2^14 = 2^138 opérations
  - Nombre d'opérations nécessaires en utilisant Pollard
    - 2^(n/3) / 1000 ≈ 2^(n/3-10)
  - Taille de clés minimum :
    - n/3 – 10 > 138
    - Donc n > 444 bits

Exercice de crypto

- Réponse question 3 :
  - Les humains devront utiliser une clé d'au moins 444 bits au lieu de 90 bits
  - Ils devront donc pratiquement quintupler la taille de la clé

Exercice de crypto

- Question 4 : Sachant que le temps pour chiffrer/déchiffrer avec RSA est en O(n^3) où n est la taille de la clé, de combien de fois les opérations de chiffrement sont ralenties par ce rallongement de la clé ?
  - 24 fois
  - 48 fois
  - 96 fois
  - 120 fois

Exercice de crypto

- Réponse question 4 :
  - On passe d'une clé de 90 bits à une clé de 444 bits
  - 444 / 90 ≈ 4,93
  - 4,93 ^3 ≈ 120
  - Les opérations de chiffrement/déchiffrement seront donc pratiquement 120 fois plus lentes

Exercice de crypto

- Ca se complique pour les humains !
- Les robots ont réussi à construire un ordinateur quantique qui permet de casser RSA par factorisarion en O(n^3) ou n est la longueur de la clé
- L'algorithme n'est pas encore très optimisé : il peut être exécuté en 10.n^3 opérations et l'ordinateur quantique peut exécuter jusqu'à 1000 opérations par seconde
- Pour le moment, les robots ne disposent que d'un seul ordinateur quantique

Exercice de crypto

- Question 5 : De combien de temps les humains disposent-ils pour réagir ?
  1. 10 minutes
  2. 10 heures
  3. 10 jours
  4. 10 ans

Exercice de crypto

- Réponse question 5 :
  - Nombre de machine : 1
  - Nombre d'opérations par seconde
    - 1000
  - Nombre d'opérations par heure
    - 1000 * 60 * 60 = 3 600 000
  - Nombre d'opérations nécessaires en utilisant l'ordinateur quantique pour une clé de 444 bits
    - 10 n^3 = 10 * (444^3) = 875 283 840
  - Nombre d'heures pour réagir :
    - 875 283 840 / 3 600 000 = 243,13 heures ≈ 10 jours

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercice de crypto

- Question 6 : Que peuvent faire les humains pour éviter que les robots ne les exterminent ?

Exercice de crypto

- Réponse question 6 :
  - Revenir à AES en allongeant la clé à 256 bits
    - Résiste à l'ordinateur quantique mais chiffrement symétrique
  - Utiliser un chiffrement de Vernam (masque jetable)
  - Déployer un algorithme de chiffrement post-quantique
    - Exemple : chiffrement de McEliece
    - Mais longueur de la clé beaucoup plus longue
    - Pas d'assurance qu'il n'y pas d'autres vulnérabilités
  - Utiliser un algorithme de cryptographie quantique

Exercice de crypto

- Exercice 2 : El gamal
  - Pourquoi : $D(y_1, y_2) = x$?
- Réponse
  - $D(y_1, y_2) = y_2 / y_1^d \bmod p$
  - $y_1 = g^k \bmod p$
  - $y_2 = xe^k \bmod p$
  - $e = g^d \bmod p$
- Donc :
  - $D(y_1, y_2) = x\,(g^d)^k \bmod p \,/\, (g^k)^d \bmod p = x$ (si $x \in Z_p^*$)