HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Enzo Allemano

07/06/2022

Duc Alexandre
Fortunato Filipe

Cryptographie

Rapport laboratoire 3:
Cryptographie asymétrique

Circuit multiplicatif corrompu

Question 1

Le y suivant retournera une valeur différente de son carré.

$$y = \ \ldots \ || \ \alpha \ || \ \beta \ || \ \ldots$$

Il faut que α et β compose y d'une quelconque manière. De cette façon, α et β seront multipliés entre eux à un moment donné et alors un nombre aléatoire sera retourné par la fonction mult.

La multiplication se faisant 32 bits par 32 bits, alors peu import la place de α et β, il y aura forcément un moment où une multiplication sera effectuée entre les deux.

Question 2

Le y^*suivant retournera une valeur correct pour p et une valeur incorrect pour q.

Pour $y^* > p$ alors $y_p = y^* \ mod \ p$ donnera une valeur élevé au carré correct

Pour $y^* < q$ alors $y_q = y^* \ mod \ q = y^*$donnera une valeur élevé au carré incorrect, car y^* restera inchangé. Cela veut dire que la condition définie à la question 1 reste vérifiée.

Il faut donc que y^* vérifie la règle de la question 1 et qu'il soit compris dans les bornes suivantes :

$$y^* \in \ [2^{511} + 2^{509}, 2^{511} + 2^{510}[$$

Question 3

Avec l'algo «square and multiply», la valeur y^* sera obligatoirement mise au carré à un moment. Ce qui veut dire que α et β seront forcément multipliés entre eux à un moment donné.

Pour $y^{*^2} mod \ p$, la valeur élevé au carré sera toujours correct

Pour $y^{*^2} mod \ q$, la valeur élevé au carré sera toujours incorrect

Question 4

Approche trivial avec les indices

$$x \equiv x' \ mod \ p \text{ et } x \not\equiv x' \ mod \ q$$

On prend $p = 7$ et $q = 17$ et donc $n = 119$

On obtient :

$$8 \ mod \ 7 \ = \ 1$$
$$15 \ mod \ 7 \ = \ 1$$

Et

$$8 \ mod \ 17 \ = \ 8$$
$$15 \ mod \ 17 \ = \ 15$$

Et pour finir :

$$15 - 8 \ mod \ 7 \ = \ 0$$

Approche concrète

Trouver ce modulo égal à zéro nous montre que nous avons trouvé un multiple de p, et donc que $x - x'$ est un multiple de p.

On a donc une première équation :

$$x - x' = k * p$$

Puisque l'on connait également la clé publique $(e1, N1)$ de la smartcard. On peut déduire l'équation suivante :

$$N1 = q * p$$

On a donc les deux équations suivantes :

$$x - x' = k * p$$

$$N1 = q * p$$

On peut donc calculer $pgcd(x - x', N1)$ pour trouver p puisqu'on sait qu'il est commun aux deux équations.

Comment trouver $x - x'$

Premièrement il faut créer un y^* qui vérifie les règles définies précédemment.

Nous allons ensuite demander à la smartcard de déchiffrer notre y^*. On peut remarquer qu'a chaque requête, la smartcard nous retourne un plaintext différent. C'est la preuve que notre y^* est correctement construit pour utiliser notre backdoor.

Il nous suffit de récupérer deux plaintext issu de y^* pour ensuite les soustraire.

Cette implémentation fonctionne grâce à la propriété d'isomorphisme des anneaux. En effet, le calcul de ${y^*}^d$ dans Z_{N1} se transforme en ${y^*}^d mod\ p$, ${y^*}^d\ mod\ q$ dans $Z_p \times Z_q$ (à l'aide de CRT^{-1}). On obtient donc un couple de valeur du style $(0, \text{multiple de p aléa.})$. Ce qui nous retourne un x, une fois que l'on a appliqué CRT.

Il suffit de répéter cette opération pour obtenir un autre x, donc un x'.

On a donc $pgcd(x - x', N1) = p$

Une fois p récupéré, les autres variables inconnues se trouve à l'aide des équations suivantes :

$$q = \frac{N1}{p}$$

$$\varphi(N1) = (p - 1)(q - 1)$$

$$d = e1^{-1}\ mod\ \varphi(N1)$$

Vérifications

$$N1 = p * q$$

$666^d\ mod\ N1$ = déchiffrement de 666 de la smartcard

Question 5

Ce challenge nous montre un exemple concret d'anneau isomorphe. On a donc une opération de mise à la puissance d'un nombre qui a lieu dans $Z_p \times Z_q$ et dans dans Z_{n}. Ceci nous permet une attaque tel que décrit dans les points précédents.

L'implémentation de ce challenge est très intéressante et m'a aidé à comprendre la matière du cours.

El Gamal sur une Courbe Elliptique

Déchiffrement

En connaissant la méthode de déchiffrement $\left(kG, M \oplus H(kA)\right)$ on peut faire la déduction suivante :

$$C = m \oplus H(kA) \text{ et } A = aG$$

$$C = m \oplus H(kaG)$$

$$C \oplus H(kaG) = m \oplus \cancel{H(kaG)} \oplus \cancel{H(kaG)}$$

$$C \oplus H(kaG) = m$$

Analyse

La première valeur de la paire retournée par la fonction de chiffrement est $u2 = kG$.

Puisque la valeur G est connue et utilisée pour tous les chiffrements avec l'EC P256 , l'approche bruteforce est clairement envisageable.

Il suffit donc de chercher une valeur de k et de multiplier par G pour retrouver $u2$.

Une fois $u2$ retrouver et k identifié, on calcul $C \oplus H(kA) = m$

Mauvaise utilisation d'RSA

Analyse

On sait que e_{31} et e_{32} sont issus du même module RSA n_3.

On peut très vite vérifier que $gcd(e_{31}, e_{32}) = 1$

Selon la théorie vu en cours :

Théorème (Inverse Modulaire)

a **est inversible modulo** *m* **si et seulement si** $\mathrm{pgcd}(a, m) = 1$.

on sait maintenant que e_{31} et e_{32} sont inversibles. On peut donc calculer $xgcd(e_{31}, e_{32})$ pour trouver l'identité de Bézout correspondante.

On connaît donc e_{31}^{-1} et e_{32}^{-1} de $e_{31} \cdot x + e_{32} \cdot y = 1$

Première approche incorrect

Les deux messages ayant été chiffrés de cette manière :

$$c_{31} = m^{e_{31}} \ mod \ n_3 \text{ et } c_{32} = m^{e_{32}} \ mod \ n_3$$

J'ai premièrement pensé à simplement calculer m en élevant un des messages chiffrés avec sont inverse. Par exemple :

$$c_{31}^{e_{31}^{-1}} = m^{e_{31} \cdot e_{31}^{-1}} = \ m \ mod \ n_3$$

Cette approche est fausse et ne fonctionne pas car e_{31}^{-1} ne correspond pas à $xgcd(e_{31}, \varphi(n_3))$.

En résumé, $e_{31}^{-1} \neq d_{31}$

Seconde approche correct

Cette fois si, je me suis tourné vers une approche qui utilise l'identité de Bézout entière tel que décrite au point de l'analyse.

Il faut donc multiplier les deux textes chiffrés pour pouvoir retrouvé l'identité dans l'exposant :

$$c_{31}^{e_{31}^{-1}} \cdot c_{32}^{e_{32}^{-1}} = m^{e_{31} \cdot e_{31}^{-1}} \cdot m^{e_{32} \cdot e_{32}^{-1}} = m^{e_{31} \cdot e_{31}^{-1} + e_{32} \cdot e_{32}^{-1}} = m^1 \ mod \ n_3 = m$$