Enzo Allemano

07/06/2022

Duc Alexandre

Fortunato Filipe

**Cryptographie**

**Rapport laboratoire 3:**

**Cryptographie asymétrique**

# Circuit multiplicatif corrompu

## Question 1

Le suivant retournera une valeur différente de son carré.

Il faut que et compose d’une quelconque manière. De cette façon, et 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 et , il y aura forcément un moment où une multiplication sera effectuée entre les deux.

## Question 2

Le suivant retournera une valeur correct pour et une valeur incorrect pour .

Pour alors donnera une valeur élevé au carré correct

Pour alors donnera une valeur élevé au carré incorrect, car restera inchangé. Cela veut dire que la condition définie à la question 1 reste vérifiée.

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

## Question 3

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

Pour , la valeur élevé au carré sera toujours correct

Pour , la valeur élevé au carré sera toujours incorrect

## Question 4

### Approche trivial avec les indices

et

On prend et et donc

On obtient :

Et

Et pour finir :

### Approche concrète

Trouver ce modulo égal à zéro nous montre que nous avons trouvé un multiple de, et donc que est un multiple de .

On a donc une première équation :

Puisque l’on connait également la clé publique de la smartcard. On peut déduire l’équation suivante :

On a donc les deux équations suivantes :

On peut donc calculer pour trouver puisqu’on sait qu’il est commun aux deux équations.

### Comment trouver

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

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

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

Cette implémentation fonctionne grâce à la propriété d’isomorphisme des anneaux. En effet, le calcul de dans se transforme en dans ( à l’aide de ). On obtient donc un couple de valeur du style . Ce qui nous retourne un , une fois que l’on a appliqué .

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

On a donc

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

### Vérifications

déchiffrement de 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 et dans dans . 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 on peut faire la déduction suivante :

et

## Analyse

La première valeur de la paire retournée par la fonction de chiffrement est .

Puisque la valeur 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 et de multiplier par pour retrouver .

Une fois retrouver et identifié, on calcul

# Mauvaise utilisation d’RSA

## Analyse

On sait que et sont issus du même module RSA .

On peut très vite vérifier que

Selon la théorie vu en cours :

Graphical user interface, application

Description automatically generated

on sait maintenant que et sont inversibles. On peut donc calculer pour trouver l’identité de Bézout correspondante.

On connaît donc et de

## Première approche incorrect

Les deux messages ayant été chiffrés de cette manière :

et

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

Cette approche est fausse et ne fonctionne pas car ne correspond pas à .

En résumé,

## 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 :