Pablo Rauzy
pr@up8.edu
https://pablo.rauzy.name/teaching/sese

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

Sécurité et systèmes embarqués

Université Paris 8 – Vincennes à Saint-Denis
UFR MITSIC / M1 informatique

Séance 4 (TP) : Cryptanalyse linéaire

N'oubliez pas :
- Les TPs doivent être rendus par courriel au plus tard la veille de la séance suivante avec "[sese]" suivi du numéro de la séance et de votre nom dans le sujet du mail, par exemple "[sese] TP4 Rauzy".
- Quand un exercice demande des réponses qui ne sont pas du code, vous les mettrez dans un fichier texte `reponses.txt` à rendre avec le code.
- Le TP doit être rendu dans une archive, par exemple un tar gzippé obtenu avec la commande `tar czvf NOM.tgz NOM`, où `NOM` est le nom du répertoire dans lequel il y a votre code (idéalement, votre nom de famille et le numéro de la séance, par exemple "rauzy-tp4").
- Si l'archive est lourde (> 1 Mo), merci d'utiliser `https://bigfiles.univ-paris8.fr/`.
- Les fichiers temporaires (si il y en a) doivent être supprimés avant de créer l'archive.
- Le code doit être proprement indenté et les variables, fonctions, constantes, etc. correctement nommées, en respectant des conventions cohérentes.
- Le code est de préférence en anglais, les commentaires (si besoin) en français ou anglais, en restant cohérent.
- **N'hésitez jamais à chercher de la documentation par vous-même sur le net!**

Dans ce TP :
- Implémentation d'un cryptosystème simple.
- Cassage de ce cryptosystème par cryptanalyse linéaire.

Exercice 0.

Recommandations.

1. Ce TP est à faire en Python.
2. Faites les questions dans l'ordre et pensez à tester votre code.
3. N'hésitez jamais à rajouter de la sortie de debug pour comprendre tout ce qui se passe.

Exercice 1.

Implémentation d'un cryptosystème jouet.

1. Notre cryptosystème, que nous appellerons *ToyCipher*, est un réseau de substitutions-permutations à deux tours, avec une clef de 8 bits et une taille de bloc (message) de 4 bits.
   La clef (k) est coupée en deux parties de 4 bits (k_0, k_1) servant de clef de tour.
   Chaque tour consiste en l'ajout de la clef correspondante à l'état (avec un `xor`), puis au passage de l'état à travers une boîte S.
   La boîte S est la suivante :

n	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(n)$	9	b	c	4	a	1	2	6	d	7	3	8	f	e	0	5

   → Implémentez la fonction de tour.
2. → Implémentez l'algorithme de chiffrement.
3. On aura besoin plus tard de la boîte S inversée.
   → Ajoutez-la dans votre code.

Exercice 2.

Comprendre la nécessité de la cryptanalyse linéaire.

1. Pour commencer, réduisons le nombre de tour de ToyCipher à un.
   (a) → Quelle type d'attaque permet de casser trivialement le chiffrement dans ce cas là ?
   (b) → Comment ?
2. Repassons donc à deux tours.
   Il ne suffit pas pour casser l'algorithme de chiffrement de répéter deux fois l'opération de la question précédente.
   → Pourquoi ?
3. Si on connaissait la clef du premier tour, on pourrait calculer la sortie du premier tour — qu'on appellera dorénavant t — et ensuite faire notre attaque de la question 1 sur le second tour.

(a) Il y a un nombre raisonnable de clef de tour possible.
→ Combien ?

(b) → Est-il pour autant possible de simplement toutes les essayer pour trouver la clef du premier tour ? Pourquoi ?

4. Sur notre exemple jouet, il serait raisonnable de faire une attaque par force brute sur la clef complète, mais ce n'est pas possible sur un vrai cryptosystème qui utilise une clef plus grande.
→ Si on définit "une étape" comme l'exécution d'un tour de notre algorithme de chiffrement, combien d'étapes sont nécessaires au maximum pour attaquer ToyCipher par force brute ? Justifiez votre réponse.

5. C'est important d'être rigoureu·x/ses ! Mettons donc en pratique la méthode scientifique.
À la question précédente, nous avons formulé une *hypothèse réfutable* concernant le nombre d'étapes nécessaires au maximum pour attaquer ToyCipher par force brute.
Cette hypothèse, qu'il nous est maintenant interdit de changer, correspond en fait à une méthode d'attaque : si on met en œuvre la méthode à laquelle vous avez pensé pour formuler votre hypothèse, on fera bien ce nombre là d'étapes (ou alors vous vous êtes complètement mélangé les pinceaux !).
La question est : est-ce que cette hypothèse est la bonne ? C'est à dire : si on met en œuvre la méthode correspondante, est-ce qu'on est sûr de trouver la bonne clef ?
On peut y répondre car l'hypothèse est réfutable : il existe un moyen de tester si elle est fausse, et dans notre cas il s'agit d'exhiber un cas où il faut strictement plus que le nombre d'étapes supposé maximum par l'hypothèse pour trouver la clef (ou alternativement, qu'on ne trouve pas la clef en ce nombre d'étape supposé maximum).

(a) → Mettez rapidement en œuvre la méthode à laquelle vous avez pensé pour formuler votre hypothèse.

(b) → Que remarquez vous ?

(c) → Si jamais votre hypothèse est réfutée, pourquoi ?

(d) → Si nécessaire, rerépondez à la question 4.

6. La cryptanalyse linéaire est une attaque à clair connue (KPA). On aura donc besoin d'un certains nombres de paires message et chiffré correspondant.
→ Écrivez une fonction qui étant donné une clef et un nombre n de paire à générer, renvoie une liste de n paires de message aléatoirement choisi et du chiffré correspondant avec la clef donnée.

Exercice 3.

Approximation linéaire de la boîte S.

1. Supposons maintenant qu'il n'est pas raisonnable d'attaquer ToyCipher par force brute. Il nous faut donc trouver un moyen plus intelligent d'attaquer notre algorithme de chiffrement.
En l'occurrence, on voudrait un moyen de deviner intelligemment des valeurs probables pour k_0, puisqu'on a vu que cela nous aiderait beaucoup à retrouver k_1.
L'idée de la cryptanalyse linéaire est d'approximer aussi bien que possible ce qu'on cherche par une fonction linéaire pour pouvoir faire des estimations éclairées par notre approximation.
Grosso-modo (en ce qui nous concerne, en tant qu'informaticien·nes), une fonction linéaire, c'est une fonction suffisamment "simple" pour nous permettre par observation de deviner ce qui se passe dedans, au sens où on est capable de dire que si l'entrée de la fonction a une propriété X, alors on sait que la sortie a une propriété Y.
Par exemple, la fonction $f : x \mapsto x + 1$ même si on ne pouvait l'utiliser qu'en boite noire, on pourrait en extraire la propriété que si son entrée en paire, alors sa sortie est impaire, et vice-versa.
Cependant, on sait que sauf faille majeur dans la conception de notre cryptosystème, notre fonction de tour n'est pas linéaire.
→ Pourquoi ?

2. On cherche donc à approcher notre fonction de tour par une approximation linéaire. La propriété que l'on va utiliser est la parité binaire des nombres en entrée et en sortie de la boîte S. La parité binaire d'un nombre est la parité du nombre de bits à 1.
Si notre boîte S n'est pas trop mal faite (et c'est le cas), on aura pas de propriété intéressante (comme une égalité, par exemple) directement. En revanche, on peut regarder si ce n'est pas le cas pour un sous-ensemble des bits.
On cherche donc deux valeurs $mask_i$ et $mask_o$ telles que si on masque l'entrée de la boîte S avec $mask_i$ (avec un `and` bit à bit, pour sélectionner seulement un sous-ensemble des bits), la parité du résultat soit la même que celle de la sortie de la boîte S masquée avec $mask_o$.
→ Écrivez une fonction qui calcule pour chaque couple $(mask_i, mask_o)$, pour combien des 16 paires entrée/sortie de la boîte S on a une égalité de parité.

3. On veut maintenant choisir la meilleure paire $(mask_i, mask_o)$. Cette paire doit évidemment faire partie de celles qui ont eu le plus haut score à la question précédente, et on veut choisir celle qui prend le plus de bits en compte (donc avec le plus de 1 dans l'écriture binaire des masques, et on exclue évidemment les masques à 0).

   → Écrire une fonction qui trouve la meilleure paire $(mask_i, mask_o)$ de masques en se basant sur le tableau de score de la question précédente.

Exercice 4.

Trouver des candidats pour k_0.

1. Maintenant que nous avons une approximation linéaire et notre boîte S, nous allons nous en servir pour trouver des valeurs potentielles de k_0.

   Pour cela on va avoir besoin d'un certains nombre de paires de message et chiffré correspondant.

   → En utilisant votre fonction de la question 6 de l'exercice 2, générez 16 paires de message/chiffré connues.

2. On veut maintenant attribuer un score à chacun des k_0 possibles.

   Pour chaque k_0 possible, pour chaque paire (m, c) de message/chiffré connue, on calcule t le résultat du premier tour de chiffrement de m avec ce k_0, et on vérifie ensuite si l'approximation linéaire de notre boîte S permet de valider le second tour. C'est à dire si notre égalité de parité binaire tient entre t et c.

   Cependant attention, c a été `xor`é (avec le vrai k_1) avant de passer dans la boîte S. Le `xor` étant une opération linéaire il ne changera pas fondamentalement notre propriété, mais il peut inverser la parité binaire et on peut donc se retrouver a devoir compter les inégalités plutôt que les égalités.

   Par exemple, si notre approximation linéaire marche dans 14 cas sur 16, il se peut qu'avec l'ajout de la clef, elle ne marche plus que dans 2 cas sur 16.

   On cherche donc une fonction de score qui maximise dans les deux cas (celui où on a beaucoup de cas qui marche, et celui ou on en a très peu).

   → Avez vous une idée de telle fonction ?

3. Les candidats qu'on retient pour k_0 sont tous ceux qui obtiennent le plus grand score de la question précédente.

   → Écrivez une fonction de sélection de candidats pour k_0. Cette fonction prend en entrée la liste des paires message/chiffré connues, et les $mask_i$ et $mask_o$ sélectionnés précédemment.

Exercice 5.

Attaque par cryptanalyse linéaire.

1. Nous avons maintenant tous les ingrédients pour monter notre attaque.

   Pour chacun des candidats k_0, on peut facilement retrouver un potentiel k_1 correspondant.

   → Comment ?

2. On a maintenant une paire (k_0, k_1) candidate à être la clef de chiffrement.

   → Écrivez la fonction qui, étant donné les k_0 candidats, trouve la clef (si possible).

3. → Branchez maintenant tout ce que vous avez écrit ensemble et vérifiez que votre attaque fonctionne.

Exercice 6.

Analyse.

1. → Combien d'étapes de calcul sont nécessaires avec l'attaque par cryptanalyse linéaire (pour la même définition d'"étape" qu'à la question 4 de l'exercice 1).
2. Comparez ce nombre avec l'attaque par force brute.

   → Qu'en dites-vous ?

3. → Pensez-vous que les calculs nécessaires pour l'approximation linéaire de la boîte S doivent être compté dans la complexité de l'attaque ? Pourquoi ?
4. → Pouvez-vous proposer une boîte S mieux conçue qui résisterait mieux à cette attaque ? Essayez avec votre code.