Licence 3 – Arithmétique et Cryptologie
2024/2025

Université de Bordeaux

Feuille 1 : Cryptographie

Exercice 1. Cryptographie hybride

Alice et Bob veulent communiquer ensemble, de façon bidirectionnelle. Bob dispose d'une clef publique K_{pub} et d'une clef privée K_{priv} pour un système de chiffrement asymétrique. On suppose qu'Oscar peut intercepter tous les messages échangés par Alice et Bob.

1. Rappeler comment Alice peut envoyer un message m à Bob sans que l'adversaire Oscar ne connaisse le message m. Quel est le concept atteint ? Quels sont les inconvénients de cette solution ?
   Alice prend la clé publique de Bob qu'on appelle K_p et un message (plain). Elle crypte m avec la clé publique de Bob, i.e., $E(m, K_p) = c$. Alice l'envoi à Bob. Puis c'est à Bob de décrypter c avec sa clef privée. Le concept atteint par cette méthode s'appelle confidentialité. Le fait que c'est pour l'instant dans un seul sens ralentira la communication entre Alice et Bob
2. Que faudrait il faire pour que Bob envoie des messages à Alice non connus d'Oscar ? Combien de clefs sont nécessaires pour que la communication se fasse dans les deux sens ? Pour que Bob envoi aussi des messages à Alice. il faut qu'Alice génére une paire de clefs (K_p^A, K_s^A).
3. Alice et Bob souhaitent utiliser un système hybride pour le chiffrement (c'est à dire qui utilise à la fois le système de chiffrement asymétrique mais également un système symétrique). Montrer comment Alice et Bob peuvent communiquer de manière sûre dans les deux sens. Quelles sont les avantages de cette solution ?
   Composantes d'un cryptosystème hybride

   (a) chiffrement symétrique : On utilise la même clef pour chiffrer et déchiffrer ;
   (b) chiffrement asymétrique : On utilise une paire de clef (K_p, K_s).

   Alice génère une clef K_{sym} et utilise la clé publique K_p de Bob. Bob le déchiffre avec sa clef prive. Donc maintenant Bob peut chiffrer ses messages avec K_{sym}. Les avantages de cette méthode sont qu'un seul couple de clef publique/privée nécessaire. Cette méthode permet de communiquer dans les deux sens et rapide.
4. On suppose maintenant qu'Oscar est capable de modifier les messages échangés par Alice et Bob. De plus, Oscar a réussi à intercepter la clef K_{pub} de Bob avant qu'Alice ne la connaisse. Montrer comment Oscar peut briser la confidentialité du système hybride de la question précédente sans qu'Alice et Bob ne s'en rendent compte. Comment pourrait on éviter cette attaque ?
   Pour éviter ce genre d'attaque, il faut relier Bob et sa clef publique, ce genre de processus s'appelle certificat. Ou peut que Bob doit remettre à Alice en main propre.

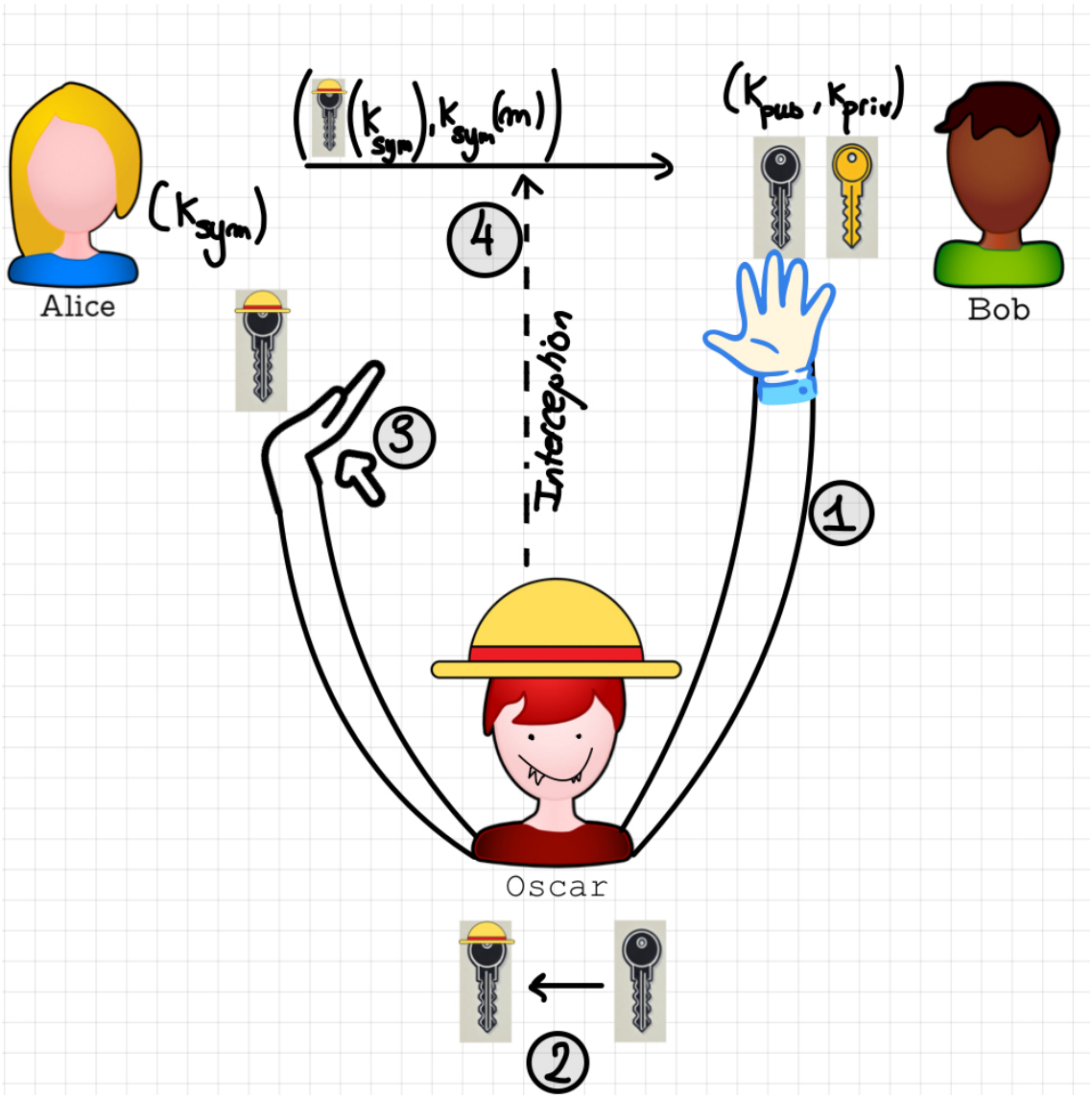

FIGURE 1 – Men in the middle

Exercice 2. La recherche exhaustive

Alice et Bob utilisent un système de chiffrement symétrique pour communiquer entre eux. Ce système de chiffrement permet d'utiliser des clefs de 64 bits, 128 bits ou de 256 bits. Alice et Bob se servent d'une clef secrète de 64 bits. Oscar dispose d'un message clair m et du chiffré c de m par ce système de chiffrement. On suppose qu'Oscar utilise un ordinateur capable d'exécuter l'algorithme de chiffrement 2^{40} fois par seconde.

1. Décrire une méthode permettant à Oscar de retrouver la clef secrète utilisée par Alice et Bob. Combien de temps lui faut il ?
   Oscar peut utilise la méthode de recherche naïve, c'est à dire de tester toutes les possibilités. Il suffit de faire un produit en croix. On obtient $2^{24}s$, ce qui fait plus de 194 jours.
2. Alice et Bob avertis de cette attaque décident d'utiliser une clef de 128 bits. Qu'en pensez vous ? Suffit de refaire le même genre de calcul. Cela prendrai plus de $2^7 1$ jours pour trouver le bon résultat.

Exercice 3. Chiffrement parfait

Un système de chiffrement est dit parfait si la connaissance d'un message chiffré n'apporte aucune information sur le message clair même à un adversaire ayant des ressources calculatoires illimités.

On considère le système de chiffrement symétrique suivant : pour échanger un message $m \in \{0, 1, 2\}$, Alice et Bob se rencontrent et décident d'une clé aléatoire $k \in \{0, 1, 2\}$ partagée. L'opération de chiffrement consiste à représenter k et m en base 2 avec 2 bits et à effectuer le « XOR » des deux représentations.

1. Quel est l'algorithme de déchiffrement ?
   Il suffit de refaire un XOR avec la clé k.
2. Faire un tableau de tous les chiffrés possibles. Ce système de chiffrement est-il parfait ?
   Le chiffrement n'est pas parfait puisque si le chiffré était 11, alors le clair ne peut pas être 00.

Un carré latin d'ordre 3 est un tableau de nombres possédant 3 lignes et 3 colonnes. Les éléments de ce tableau appartiennent à l'ensemble $\{0, 1, 2\}$ et sont tels que chaque nombre de cet ensemble n'apparaît qu'une seule fois sur chaque ligne et chaque colonne. On note $l_{i,j}$ l'élément situé en ligne i et colonne j. On modifie le système de chiffrement de la manière suivante : le chiffré du message $m \in \{0, 1, 2\}$ avec la clef $k \in \{0, 1, 2\}$ est l'élément l_{km}.

3. Donner un exemple de tel carré latin.

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

4. Quel est l'algorithme de déchiffrement ? Le système de chiffrement est-il parfait ? On examine la ligne k pour trouver l'occurrence unique de $c = l_{km}$. C'est un chifffrement parfait puisque pour chaque texte chiffré, tout message initial est possible.

Exercice 4. Chiffrement par substitution

Soit σ une permutation de $\mathbf{Z}/26\mathbf{Z}$. Chaque lettre de l'alphabet est identifiée à un élément x de $\mathbf{Z}/26\mathbf{Z}$ et est chiffré $\sigma(x)$.

1. Comment chiffre-t-on et déchiffre-t-on un message ? Combien a-t-on de clés différentes possibles ? Comparer avec le nombre de clés différentes possibles dans le cas du chiffrement par décalage. Pour chiffrer un message, on prend un élément de $\sigma \in \mathcal{S}_{26}$ et on applique au message clair $x \in \mathbf{Z}/26\mathbf{Z}$ c'est à dire $\sigma(x)$. Pour déchiffrer, on peut appliquer la permutation inverse σ^{-1} puisque $\sigma^{-1}\sigma(x) = x$. Donc nous avons $E(x, \sigma) = \sigma(x)$ et $D(y, \sigma) = \sigma^{-1}(y)$. Le nombre de clés différentes possibles est déterminé par le cardinal du groupes de permutations à 26 éléments qui est 26!. Et le nombre de clés différentes possibles dans le cas du chiffrement par décalage est juste 26.
2. Montrer que l'application $x \mapsto x^5$ ne définit pas une permutation de $\mathbf{Z}/31\mathbf{Z}$, mais que $x \mapsto x^7$ si, et déterminer la fonction de déchiffrement (on admet le petit théorème de Fermat, qui implique en particulier que $x^{30} \equiv 1 \mod 31$ pour tout entier x non divisible par 31). Une permutation est juste une bijection d'ensemble. Donc il suffit soit montrer qu'elle n'est pas injective ou surjective. Prenons par exemple 1 et 2, $1^5 = 1 = 32 = 2^5 \mod 31$. l'application n'est pas injective et donc pas une permutation. Maintenant montrons que $x \mapsto x^7$ est une permutation dans $\mathbf{Z}/31\mathbf{Z}$. On sait que l'application $x \mapsto x^k$ pour $k \in \{0, 1, \ldots, 30\}$ est bijective si et seulement si $\text{pgcd}(k, 30) = 1$. Ce qui est le cas pour 7 mais pas pour 5.

Exercice 5. Cryptanalyse par fréquence

Le but de l'exercice est de déchiffrer le texte chiffré ci-dessous grâce à une analyse de fréquence. Le texte est en français. On utilisera le fait que la lettre la plus fréquente en français est le E, viennent ensuite S, A, T, I.

XGCLKPHEUL GPFQYYWHST YIYHFENYIG HFYIGHQASY
DQWGTHGWYC SLQWYLXYWC EIISTQCGHQ ETWTSIYLQA
SYW

1. Si, comme on peut s'y attendre, la lettre la plus fréquente du message clair est le E, peut-on affirmer que le message a été chiffré par décalage ?
   - **Y** : 12 occurrences
   - **G** : 7 occurrences
   - **H** : 7 occurrences
   - **Q** : 7 occurrences
   - **W** : 7 occurrences
   - **S** : 6 occurrences
   - **I** : 6 occurrences
   - **L** : 5 occurrences
   - **T** : 5 occurrences
   - **C** : 4 occurrences
   - **E** : 4 occurrences

— **F** : 3 occurrences
— **X** : 2 occurrences
— **P** : 2 occurrences
— **A** : 2 occurrences
— **K** : 1 occurrence
— **U** : 1 occurrence
— **N** : 1 occurrence
— **D** : 1 occurrence

Donc on doit décaler la lettre E vers la lettre Y dans ce cas, le message n'est toujours pas décrypté.

2. Sachant que le message a été codé à l'aide d'une application de la forme $x \mapsto ax+b$ avec x, a et b dans $\mathbf{Z}/26\mathbf{Z}$ (avec $A = \bar{0}$, $B = \bar{1}$ etc.), déchiffrer le message ci-dessus.

   On sait déjà que la lettre Y correspond à E i.e., $f(E) = f(4) = a * 4 + b = 24 = Y$. Par contre pour la lettre S, l'analyse des fréquences des lettres nous dit que $f(S) \in \{G, H, Q, W\} = \{6, 7, 16, 22\}$. Il faut donc résoudre des équation linéaires. Supposons que $f(S) = W \iff f(18) = a * 18 + b = 22$. On obtient $(a, b) = (11, 6)$ et le message décrypté est :

   LA CRYPTOGRAPHIE EST UNE METHODE MATHEMATIQUE VISANT A SECURISER LES COMMUNICATIONS NUMERIQUES