TD 2 Algorithmes de cryptographie

Ex 1 Généralités sur les crypto-systèmes :

On définit un *crypto-système* comme un tuple (*P, C, K, E, D*), où :

- *P* est l'ensemble des *textes en clair*,
- *C* est l'ensemble des *textes chiffrés*,
- *K* est l'ensemble des *clefs*,
- $E = \{e_k, k \in K\}$ est l'ensemble des fonctions de chiffrement, $e_k : P \rightarrow C$,
- $D = \{d_k, k \in K\}$ est l'ensemble des fonctions de chiffrement, $d_k : C \rightarrow P$,
- Pour tout $k \in K$, il existe k' tel que $d_{k'}(e_k(p)) = p$ (pour tout $p \in P$)

1. On considère le système de *César* défini comme suit :
   - $P = C = K = \Sigma = \{A, B, \ldots, Z\}$,
   - on identifie les lettres avec les entiers, A avec 0, B avec 1, …, Z avec 25,
   - $e_k : \Sigma \rightarrow \Sigma$, est définie par $x \rightarrow (x+k) \bmod 26$,
   - $d_k : \Sigma \rightarrow \Sigma$, est définie par $x \rightarrow (x-k) \bmod 26$,
   - les clefs de chiffrement et de déchiffrement sont identiques,
   - le chiffrement d'une séquence de lettres de Σ est obtenu en concaténant les chiffres de chacune des lettres de la séquence.

   On sait que le texte chiffré VHFUHW a été généré avec le crypto-système précédent. Déterminer la clef et le texte en clair correspondant.

2. Montrer que les fonctions de chiffrement d'un crypto-système sont toujours injectives.

3. On considère les systèmes suivants ($\Sigma = Z26$) :
   a. $P = C = \Sigma$, $k \in \{1,2, \ldots, 26\}$, e_k est définie par $x \rightarrow (k*x) \bmod 26$,
   b. $P = C = \Sigma$, $k \in \{1,2, \ldots, 26\}$ *et* $pgcd(k,26)=1$, e_k est définie par $x \rightarrow (k*x) \bmod 26$.

   Dire pour chacun s'il s'agit d'un crypto-système (justifier).

4. On considère l'alphabet privé de la lettre W (soit 25 lettres). Polybe (200-125 avant J.C.) a proposé le chiffrement qui suit : on range les lettres de l'alphabet dans un carré de taille 5*5 en commençant par un mot clé et en continuant avec les lettres restantes de l'alphabet (en supprimant les doublons). Par exemple, avec le mot clé MYSTERE on obtient le tableau suivant :

	1	2	3	4	5
1	M	Y	S	T	E
2	R	A	B	C	D
3	F	G	H	I	J
4	K	L	N	O	P
5	Q	U	V	X	Z

   Le chiffrement s'effectue alors en remplaçant chaque lettre par les deux chiffres indiquant sa ligne et sa colonne. Par exemple, S est chiffré par 13.

(a) Expliquer comment peut-on cryptanalyser un tel système par une attaque à clair connu puis par une attaque simple (avec seulement un chiffré).

(b) Raoul envoie un message à Ánna pour lui fixer un rendez-vous. Le cryptogramme est le suivant :

```
123222  512215  424215  512242  242255  534352  111524  225254
322252  512211  515222  532251  142251  154352  21
```

Décrypter ce message !

5. Comment peut-on distinguer un réseau de Feistel à deux tours d'une fonction aléatoire ?

6. Le nombre de clés disponibles dans un système de chiffrement donne une borne maximale de sa sécurité (mesure de la complexité d'une recherche exhaustive) mais rarement une bonne mesure :
    a. Quel est le nombre de clés possibles pour un chiffrement de César ?
    b. Pour un chiffrement affine (C(x)=ax+b mod 26 pour chaque caractère dans Z_{26}) ?
    c. Pour un chiffrement par substitution (substitution arbitraire, caractère par caractère) ?
    d. Pour un chiffrement de Vigenère (avec une clé de longueur k) ?

Ex 2 Echanges sécurisées

Astrid et Béatrice veulent communiquer toute la journée en échangeant des fichiers {Fi}i. Elles connaissent la cryptographie, les algorithmes de chiffrement (RSA, AES, etc.) et la création et gestion de clés. Comment vont-elles s'y prendre pour communiquer entre elles de manière sécurisée ?

Ex 3 Force de 2DES

1. Expliquer la réalisation de 3DES (TDES). Pourquoi 3DES est utilisé en pratique au lieu de DES? Quelle est le facteur de complexité ajouté par 3DES ?
2. Pour alléger l'exécution de 3DES, on propose une alternative : 2DES. Dans 2DES, on fait une composition de deux chiffrements par DES classiques avec des clés différentes : C = 2DES(k2|k1, m) = DES(k2, DES(k1, m))
    a. Citer les avantages de cette approche par rapport à 3DES. Quelle est la première estimation naïve de la force cryptographique théorique de 2DES ?
    b. Analyse de sécurité de 2DES :
        i. Combien y a-t-il de clés différentes? Combien y a-t-il de collisions, définies comme suit : ∃ m, c | 2DES(k, m) = c = 2DES(t, m), avec k ≠ t.
        ii. Meet in the Middle attack (Diffie et Hellman, 1977) : en utilisant la propriété de DES suivante : si c = DES(k2, DES(k1, m)), alors il y a un c1 = DES (k1, m) = DES-1(k2, c) ; construire une méthode d'attaque sur 2DES en utilisant 2 paires de textes clair/chiffré.
        iii. Estimer les efforts nécessaires pour cette attaque et la probabilité d'avoir trouvé la bonne clé. Quelle est alors la force estimée de 2DES ?

Ex 4 RSA

On utilise les notations habituelles pour RSA :

p,q, n, phi, e, d, n= pq, phi = (p-1)(q-1), ed = 1 mod phi

1. Chercher l'inverse de 89 sur ℤphi avec phi=197.
2. On chiffre un message m qui devient le message c en utilisant l'algorithme de chiffrement asymétrique RSA: quelle est la formule de chiffrement ? Quelle est la formule de

déchiffrement ? Quelles sont les valeurs qui doivent rester secrètes parmi n, p, q, phi, e, d ?

3. On donne n=3001, e=3, chercher la clé d associée à e. On chiffre un message m=4, trouver le message chiffré c. Est-il possible de retrouver m à partir de c sans connaître d ? Proposer une solution ?
4. On suppose n = 65. Calculer p, q, phi. Donner tous les couples (e, d) possibles. Combien y en a-t-il ? Chiffrer le message m = 4 avec pour la clé publique e = 5. Déchiffrer le message c avec la clé privée d correspondante.

Ex 5 Vulnérabilités de RSA

L'algorithme RSA est, sous la forme de l'exercice précédent, vulnérable à de nombreuses attaques. Pour s'en convaincre, on se propose d'étudier l'une d'entre elles : montrer que le produit des signatures de deux messages (réalisées avec la même clef privée) est égal à la signature du produit des deux messages.

Ex 6 De φ(n) à la factorisation

On considère un module RSA n=pq, où p et q sont les inconnues ;

1. Montrer comment la connaissance de φ(n) (fonction d'Euler) permet de remonter à la factorisation de n.

Considérer le système RSA avec p=19 et q=23

2. Calculer n et φ(n)
3. Calculer l'exposant d associé à e=9
4. Calculer l'exposant e associé à e=17

Ex 7 Calcul Modulaire

Calculez (de tête si c'est possible)

1. $2^{256} \bmod 123$
2. $529^{436} \bmod 66$
3. $1023^{4096} \bmod 1024$
4. $456^{2308} \bmod 234327$

Ex 8 Recherche exhaustive de clefs symétriques

Sachant que la machine spécialisée « DES-Cracker» met en moyenne 4,5 jours pour retrouver par une recherche exhaustive une clef DES de 56 bits, combien de temps mettrait-elle pour trouver une clef de 40 bits ? Une clef Triple-DES de 112 bits ? Une clef AES de 256 bits ? On admettra ici que cette machine a besoin du même temps pour chiffrer un bloc de données avec DES, Triple-DES et AES.

Ex 9 Fonctions de hachage et paradoxe des anniversaires

La fonction de hachage SHA-1 génère des empreintes numériques de 160 bits. On suppose que l'on décide de créer un certificat numérique pour chaque habitant de la Terre (6×10^9) habitants.

1. Calculer la probabilité qu'au moins un certificat possède la même empreinte que le certificat de Mr. z : Ox11c42333330debe663d722a5f34388c8b88520bb
   (En notation hexadécimale), en s'aidant du fait que $1 - x \approx e^{-x}$ pour x proche de 0.

2. Calculer la probabilité qu'au moins deux habitants de la planète possèdent une empreinte identique.

Ex 10 Modes de chiffrement symétrique

Texte en clair X_i et texte chiffré Y_i. On admettra qu'on chiffre des données au moyen de Triple DES (qui chiffre des blocs de 64 bits) en mode CBC et qu'un pirate trouve deux blocs Y_i et Y_j tels que $Y_i = Yj$ et $i \neq j$. Quelle information sur le texte clair peut-on déduire de cette relation ? En supposant que l'on chiffre les données d'un disque dur avec Triple-DES en mode CBC, quelle doit être la taille du disque pour que la probabilité d'une collision soit supérieure à 40% ?

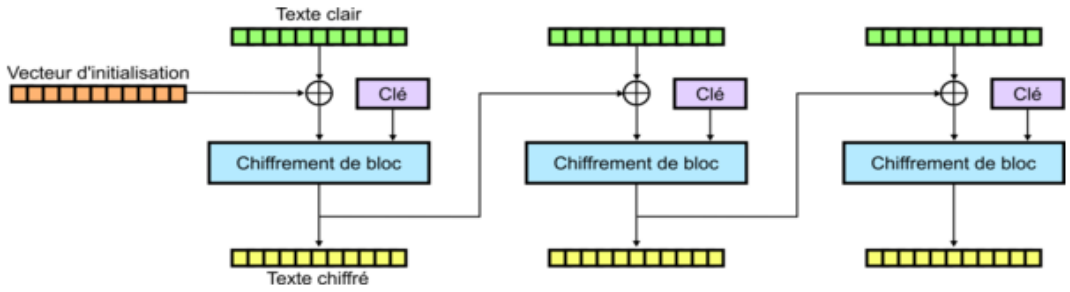


Fig. Mode de chiffrement CBC

$Y_i = Y_j$

X_i et X_j ?

Ex 11 Chiffrement symétrique et asymétrique

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre.

Le groupe décide d'utiliser un système symétrique de chiffrement.

1. Quel est le nombre minimal de clés symétriques nécessaires?
2. Donner le nom d'un algorithme de chiffrement symétrique reconnu.

Le groupe décide ensuite de remplacer ce système par un système asymétrique.

3. Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées?

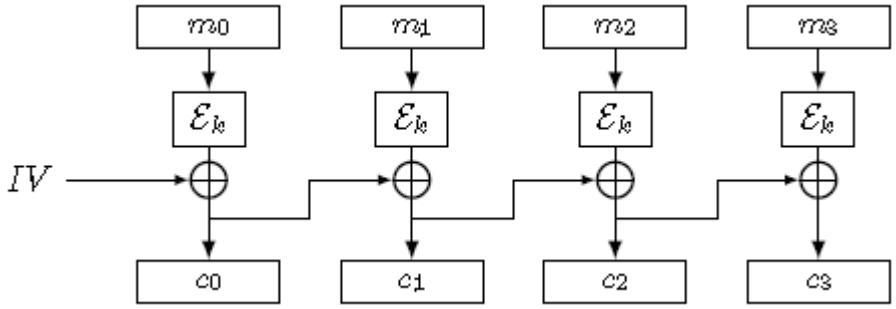
4. Bob souhaite envoyer des informations chiffrées et signées à Alice, Bob et Alice appartiennent tous les deux au groupe. Quelle clé doit utiliser Bob?
5. Donner le nom d'un algorithme de chiffrement asymétrique reconnu.

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement c'est à-dire qui utilise la cryptographie symétrique et asymétrique.

6. Donner les raisons qui ont poussé ce groupe à utiliser un tel système.

Ex 12 Mode opératoire CBC

Au lieu du mode CBC, on emploie le mode opératoire suivant un chiffrement symétrique :



Quel est le problème de ce nouveau système ?

Ex 13 Perte d'une clé privée

Alain, qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clé privée, mais dispose encore de la clé publique correspondante.

1. Peut-il encore envoyer des courriers électroniques chiffrés? En recevoir?
2. Peut-il encore signer les courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit?
3. Que doit-il faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus?

Ex 14: Authentification de messages (MAC) par blocs

Soit un message $m=m_1||m_2||\ldots||m_n$ à authentifier avec une clef k. soit F_k une fonction pseudo-aléatoire (par exemple une fonction de chiffrement sûre). Pour authentifier le message m, on calcule le MAC suivant :

$$MAC_k(m) = F_k(m_1) \oplus \cdots \oplus F_k(m_n)$$

1. Expliquer pourquoi ce calcul ne garantit pas l'intégrité du message dès qu'il y a au moins deux blocs.
2. Montrer pourquoi il est simple pour l'attaquant d'authentifier un message de la forme m||m
3. Montrer comment l'attaquant peut authentifier n'importe quel message en posant deux questions.

Afin de contrer les attaques basiques telles que suppression ou échange de blocs, on considère le schéma suivant :

$$MAC_k(m) = F_k(1\|m_1) \oplus F_k(2\|m_2) \oplus \cdots F_k(n\|m_n)$$

4. Montrer qu'il est toujours possible d'authentifier un message arbitraire en posant trois questions.

Ex 15 RSA bis

On utilise les notations habituelles du RSA : p, q, n, phi, e, d. On note n= p.q, phi = (p-1).(q-1), e.d = 1 mod phi. On chiffre le message m qui devient le message c.

1. Astrid utilise pour clé publique : (121, 899). Écrire les formules de chiffrement et déchiffrement. Calculer p, q, phi et d. Chiffrer le message m = 2 avec la clé privée.

2. Astrid a choisi pour clé publique (121, 899). Y a-t-il d'autres solutions possibles ?
Est-ce que e = 289 et d = 529 est un couple possible de clés de chiffrement-déchiffrement ?
($289 = 17^2$; $529 = 23^2$)

3. Astrid choisit maintenant e = 13 * 17 = 221. Est-ce possible ? Si oui, calculer d. Chiffrer le message m = 2 avec la clé publique e. Déchiffrer le message c ainsi trouvé (donner la formule).

Remarque 1 : On donne les nombres premiers jusqu'à 1000.

2 3 5 7 11 13 17 19 23 29

31 37 41 43 47 53 59 61 67 71

73 79 83 89 97 101 103 107 109 113

127 131 137 139 149 151 157 163 167 173

179 181 191 193 197 199 211 223 227 229

233 239 241 251 257 263 269 271 277 281

283 293 307 311 313 317 331 337 347 349

353 359 367 373 379 383 389 397 401 409

419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013

Remarque 2 : On donne certaines exponentiations modulaires de 2.

$2^{120} \bmod 899 = 807$

$2^{360} \bmod 899 = 745$

$2^{121} \bmod 840 = 632$

$2^{361} \bmod 840 = 632$

$715^{360} \bmod 899 = 342$

$715^{121} \bmod 899 = 591$

$2^{220} \bmod 899 = 745$

$591^{821} \bmod 899 = 2$

Ex 16 Algorithme de Diffie-Hellman

Déterminer la clé de session Diffie-Hellman, si Alice communique à Bob les nombres g=3 et p=23. Sachant qu'Alice tire le nombre aléatoire a=5 et Bob le nombre b=7 ?