Examen Blanc

Exercice 1 :

Rappelons la correspondance entre l'alphabet classique et les entiers {0, . . . , 25} :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Pour les exercices suivants, nous prenons le message *M* = LESMAISONSBLANCHES.

1. Soit *K* = ULOIDTGKXYCRHBPMZJQVWNFSAE une clé de substitution. En rappelant l'application induit par la clé :

ABCDEFGHIJKLMNOPQRSTUVWXYZ
↓ . . . ↓
ULOIDTGKXYCRHBPMZJQVWNFSAE

Trouver le chiffrement de *M*. Quelles propriétés du texte clair et du texte chiffré restent inchangées par un chiffrement à substitution ?

2. Trouver le chiffrement de *M* par transposition avec la clé [3,5,2,6,1,4]. Quelles propriétés du texte clair et du texte chiffré restent inchangées par un chiffrement à substitution?

3. Trouver le chiffrement de *M* par un chiffrement de Vigenère avec la clé SECURITE. Qu'est-ce se passe aux fréquences des caractères dans un texte chiffré avec un chiffrement de Vigenère ?

Solution :

1. *Le chiffrement de* LESMAISONSBLANCHES *est* RDQHUXQPBQLRUBOKDQ*. Les fréquences des caractères du texte clair et de son texte chiffré diffèrent seulement par la permutation des caractères.*
2. *Le chiffrement de M est* SAEILMNBOLSSCENSAH*. Les fréquences des caractères du texte clair et son texte chiffré sont égaux.*
3. *Le chiffrement de M est DIUGRQLSFWDFRVVLWW. La fréquence de chaque lettre du texte chiffré et une moyenne de plusieurs fréquences dans le texte clair*

Exercice 2 :

RSA Dans toute la suite, on pourra utiliser les résultats numériques suivants:

- 319 = 11 × 29; 1011 = 263 (mod 319); 2632 = 216 × 319 + 265 ;
- 1333 = 12 (mod 319); 13325 = 133 (mod 319);
- 112 = 121 (mod 280); 114 = 81 (mod 280); 118 = 121 (mod 280); 1116 = 81 (mod 280);
- 95 = 64 + 31; 81.11 = 51 (mod 280); 81.121 = 1 (mod 280).

Exercice 1 (Chiffrement/Déchiffrement RSA) On considère la clef publique RSA (11, 319), c'est à dire pour n = 319 et e = 11.

1. Quel est le chiffrement avec cette clé du message M = 100?

2. Calculer d la clé privée correspondant à la clé publique e.

3. Déchiffrer le message C = 133.

4. Le message codé 625 peut-il résulter d'un codage avec la clé publique ? Même question avec la clé privée.

Solution :

1. *M'= 100^{11} (mod 319) = 265 2.*
2. *On doit résoudre $11 * d = 1$ (mod 280). On trouve d = 51*

   • soit en utilisant l'algorithme d'Euclide étendu;

   • soit en essayant « à la main » car $51 = (280/11) * 2$ donc il suffit de deux essais pour trouver;

   • soit en utilisant Euler, $d = 11^{-1}$ (mod 280) d'où $d = 11^{\varphi(280)-1}$ (mod 280) = $11^{\varphi(7.5.8)-1}$ (mod 280) = $11^{(6.4.4)-1}$ (mod 280) = 11^{95} (mod 280) = $11^{64+16+8+4+2+1}$ (mod 280) = 81.81.121.81.121.11 = 81.11 = (mod 280) = 51 (mod 280).

3. *On doit calculer 133^{51} (mod 319). Dans les notes on donne $133^{25} = 133$ (mod 319). Le résultat est $133 * 133 * 133$ (mod 319) = 12.*
4. *4. évidemment non pour les deux car les messages à chiffrer/déchiffrer doivent appartenir à Z_n, c'est à dire Z_{319} dans ce cas.*

Exercice 3 :

Le protocole HTTPS (HTTP sur SSL/TLS) est couramment utilisé pour sécuriser les communications entre un serveur Web et un navigateur. Pour cela, une session HTTPS s'appuie sur un certificat diffusé par le serveur permettant d'effectuer une session d'authentification initiale et ensuite un chiffrement du canal de communication dans lequel transite l'échange HTTP.

1. Lors de l'authentification, le protocole utilise une clef publique contenu dans un certificat que le serveur détient et diffuse au client à l'établissement de la connexion. Quelles sont les protections offertes par cette utilisation d'un certificat serveur ?
2. Comment l'utilisateur du navigateur peut-il être assuré que cette clef publique correspond bien à l'organisme auquel il souhaite accéder ?
3. Pourquoi de nombreux services Web, utilisant pourtant HTTPS, demandent-ils en plus à l'utilisateur de fournir un nom de compte et un mot de passe pour compléter l'ouverture de session ?
4. Il est possible d'utiliser un certificat client stocké sur le navigateur pour l'échange HTTPS. Quel est l'effet de l'utilisation d'un certificat client sur la protection de l'ensemble du service ?
5. Avec un certificat client, l'utilisateur doit quand même parfois fournir une « *passphrase* »: de quel mot de passe s'agit-il ?
6. Pensez-vous qu'il y ait une « *passphase* » utilisateur sur la partie privée du certificat serveur ? Pourquoi **?**

Solution :

1. *Le protocole SSL avec un certificat serveur offre d'abord une authentification du partenaire accédé par une vérification que ce serveur détient bien la clef privée correspondant à la clef publique diffusée. Ensuite, la communication est chiffrée, on*

a donc des garanties sur la confidentialité des échanges ainsi que sur l'intégrité de la communication pendant toute sa durée.

2. *Le certificat n'inclut pas seulement la clef publique, mais également une signature de cette clef publique par un autre certificat. (Celui-ci pouvant également être un certificat intermédiaire.) La racine de cette chaîne de certification doit être un certificat pré-installé sur le navigateur (ou obtenu indépendamment en préalable à la communication). L'utilisateur peut alors être sûr que le certificat diffusé par le serveur appartient bien à l'organisme indiqué s'il vérifie la chaine de certification, s'il a confiance dans le certificat racine et s'il a confiance dans les organismes détenteurs des certificats intermédiaires pour avoir fait les vérifications nécessaires avant de signer les certificats dérivés. (Il s'agit alors de tiers de confiance ou d'autorités de certification.)*
3. *Le certificat serveur n'offre qu'une authentification du serveur. Si le service accédé gère une base de comptes utilisateurs, ceux-ci doivent donc également en plus s'authentifier. Cette authentification du client peut éventuellement s'effectuer via un nom d'utilisateur et un mot de passe. Cette méthode est moins forte qu'une technique faisant appel à des algorithmes de cryptographie asymétriques, mais elle est bénéficiée néanmoins via HTTPS de la protection offerte par le canal chiffré et signé de SSL.*
4. *Dans ce cas, l'authentification du client, appuyée sur un certificat et une authentification à clef privée/clef publique offre des garanties bien plus importantes en termes de sécurité. Par contre, il faut alors gérer une procédure de délivrance de ces certificats clients (incluant leur signature par un tiers de confiance, après vérification de l'identité du demandeur par exemple).*
5. *La clef privée associée à un certificat ne doit être que très rarement stockée en clair (notamment sur disque). Elle est protégée par un chiffrement symétrique dont la « passphrase » constitue la clef. C'est donc un mot de passe permettant de déverrouiller l'usage du certificat et de protéger la clef privée de l'utilisateur en cas de vol (par exemple afin de lui laisser le temps de détecter le vol et de révoquer son certificat).*
6. *Si une passphrase est aussi utilisée sur le serveur, à chaque lancement du service Web, il sera nécessaire de la fournir au programme afin qu'il puisse accéder à la clef privée du certificat serveur. Il est peu probable que ceci soit effectué de manière interactive (à chaque redémarrage...). Il est plus probable qu'en pratique, soit la clef privée est effectivement stockée en clair sur le serveur, soit la passphrase en question est stockée dans les paramètres de configuration du serveur (ce qui n'est pas mieux). Ce faisant, les administrateurs Web/système dérogent vis à vis du certificat serveur aux règles de protection qu'ils recommandent à leurs utilisateurs pour les certificats clients. À méditer...*