USTHB, FEI, DI **Master 1 IL**

Epreuve de Sécurité Informatique

Question 1. (4 pts). Quelles sont les idées évoquées dans le cadre des systèmes de chiffrement classiques qui ont été retenues pour la conception des systèmes de chiffrement symétriques modernes de type DES et AES ? et comment ? Expliquer la notion de système itéé qui les caractérise à l'aide des chiffrements à décalage et multiplicatif.

Solution. Cf. cours

Question 2.(**4 pts**). Le message ci-dessous (d'un auteur américain célèbre) a été chiffré par le chiffrement par décalage (ou de César). On sait de plus qu'il a été écrit en français dont on connaît la distribution de probabilités des (fréquences f) caractères dans un texte pris au hasard.

nqsdfufxijrjxxfljhmnkkwjufwqnsljsntxnyjmzrfnsjvzjqnsyjqqnljshjsjuznxxjijhmnkkwjw

lettre	a	b	c	d	e	f	g	h	i	j
f	0.081	0.009	0.023	0.077	0.145	0.010	0.005	0.053	0.077	0.005
Lettre	k	l	m	n	o	p	q	r	s	t
f	0.0001	0.051	0.017	0.063	0.043	0.028	0.008	0.053	0.038	0.063
Lettre	u	v	w	x	y	z				
f	0.053	0.009	0.0001	0.0004	0.0001	0.0002				

(i)« Casser » ce système, soit en déchiffrant le message, et trouver ainsi la clé (ou l'inverse). (ii) Combien de tentatives aurait-il fallu pour « casser « le système avec la recherche exhaustive (« attaque brute »).

Solution. On commence par trouver la loi de probabilités des caractères dans le texte chiffré : J apparaît 14 fois, N 10 fois, S 7fois, X 6 fois, F 5 fois, R et Q 4 fois…..C'est suffisant pour la suite. Première hypothèse : le J correspond au caractère E dans le clair, ce qui donne l'équation J=E+k mod 26 ou en numérique, 9=4+kmod26, soit k=5. En essayant celle clé on trouve que c'est la bonne clé car elle donne un texte qui a un sens (il n'ya

ILNYAPASDEMESSAGECHIFFREPAR LINGENIOSITEHUMAINQUE

LINTELLIGENCENEPUISSEDECHIFFRER, Edgar Allan Poe.

Question 3. (**4 pts**).Donner l'algorithme de chiffrement asymétrique RSA. (i) Quels sont à votre avis les avantages de ce type de chiffrement par rapport aux systèmes symétriques de la question 1 ? (ii) Expliquer son mode de fonctionnement : Comment le paramétrer ? Comment se font les algorithmes de chiffrement et déchiffrement (algorithme correspondants) ? (Indication : quelle est la signification et le rôle de $n, p, a, b, \varphi(n)$). (iii) Montrer comment B crée sa clé publique s'il a choisi $p = 3, q = 5,\ b = 7$. Ce paramétrage est-il correct ? Montrer comment effectuer le chiffrement du message clair I dans l'alphabet latin Z_{26} et le déchiffrement du message codé correspondant. (iv) Discuter sa sécurité : pourquoi est-il considéré comme sûr ? Indiquer quelques unes de ses failles.

Solution: (i) les DES/AES sont caractérisés par des clés courtes ; des clés longues pour RSA… ; le système à clé publique résoud en partie le problème d'échanges de clés secrètes ; les systèmes à clés secrètes ont des débits plus rapides.(ii) cf.cours ; (iii)Par B : $n = p \times q = 15, \varphi(n) = 2 \times 4 = 8, b = 7, a = 7^{-1} mod 8 = 7$

En numérique (dans Z_{26}), x est codé par 8.

Chiffrement par A :$x = 8; y := 8^7 mod 15 = 2;$ $Déchiffrement\ par\ B\ \ x = 2^7 mod 15 = 8.$

N.B. Notez que la clé de déchiffrement est la même que celle du chiffrement. Si Oscar s'en aperçoit il pourra déchiffrer tous les messages que A adressera à B, puisque la clé b=7 est publique.

Sécurité et failles (cf. cours).

Question 4. (**4 pts**). L'une des attaques (théoriques) sur le système RSA est la factorisation du modulus n. Montrer commment procéder à ce type d'attaque à l'aide de la technique (« grossière ») rho de Pollard, si $n = 247$. Expliquer le principe de cet algorithme. On choisira $a = 2, b = 5, f(x) = x^2 + 1 \ mod\ n$. Pourquoi le fait de trouver un facteur non trivial de n permet-t-il de « casser » le RSA.

Solution. **Algorithme (ρ de Pollard).**

1.Poser $a := 2, b := f(a)$. (Ici $f(x) = x^2 + 9 \bmod n$).

2. Pour $i = 1,2,...$, Faire

2.1. Calculer $a := a^2 + 1 \bmod n, b := b^2 + 1 \bmod n$.

2.2. Calculer $p := PGCD(a - b, n)$.

2.3. Si $1 < p < n$ alors p est un facteur non trivial (succès).

2.4. Si $p = n$, alors échec.

A.N. $n = 247$

a	2	5	26	183
b	5	26	183	145
$a - b$	-3	-21	-157	38
p	1	1	1	19

On a bien $247 = 13 \times 19$.

Question 5. (4 pts).Quel est l'intérêt d'utiliser l'algorithme d'exponentiation rapide dans l'implémentation du système RSA ? Rappelez cet algorithme ? Déroulez-le pour calculer $741^{33} mod 943$.

Solution. Pour chiffrer le clair et déchiffrer le crypté à l'aide de la fonction d'exponentiation modulaire. $741^{33} mod 943 = 413$, comme le montrent les calculs ci-dessous,

$33=1\times2^0+0\times2^1+0\times2^2+0\times2^3+0\times2^4+1\times2^5$

i	b_i	z
5	1	$1^2 \times 741 mod 943 = 741$
4	0	$741^2 mod 943 = 255$
3	0	$255^2 mod 9439011$
2	0	$901^2 mod 943 = 821$
1	0	$821^2 mod 943 = 739$
0	1	$739^2 mod 943 = 413$

Mai 2017