1 Protocole RSA

Génération de clefs

Alice effectue les opérations suivantes :

- Choisir deux entiers premiers p et q, calculer $n = pq$.
- Calculer $\varphi(n) = (p-1)(q-1)$ et un entier e premier avec $\varphi(n)$.
- Calculer d tel que $de = 1 \mod \varphi(n)$

Elle publie ensuite la clef publique $pk = (n, e)$ et garde secret la clef privée $sk = d$.

Exercice 1

On considère les valeurs $p = 53$, $q = 11$ et $e = 3$.

1. Calculez la valeur publique n.
2. Calculez la fonction d'Euler $\varphi(n)$.
3. Utilisez l'algorithme étendu d'Euclide pour calculer la valeur d de la clef privée.

Chiffrement

Bob veut envoyer un message à Alice. Il cherche dans l'annuaire la clef de de chiffrement qu'elle a publiée. Il sait maintenant qu'il doit utiliser le système RSA avec les deux entiers n et e. Il transforme en nombres son message en remplaçant par exemple chaque lettre par son rang dans l'alphabet. (Exemple : "JEVOUSAIME" donne 10 05 22 15 21 19 01 09 13 05) Puis il découpe son message chiffré en blocs de même longueur (en partant de la droite) représentant chacun un nombre le plus grand possible tout en restant plus petit que n.

Exercice 2

1. Que devient le message ?
2. Pourquoi ne pas garder des blocs de taille 2 ?
3. Un bloc B est chiffré par la formule $C = B^e \mod n$. Quel message obtient Bob après avoir chiffré chaque bloc ?

Déchiffrement

Alice utilise sa clef privée d.Chacun des blocs C du message chiffré sera déchiffré par la formule $B = C^d \mod n$.
Quel message retrouve Alice ?

2 Applications

Exercice 3

Connaissant la clef publique $(n = 119, e = 5)$ de ce cryptogramme RSA 7 bits (090 086 036 067 032 001 003 031 059 031)

1. Calculez (par tout les moyens à votre disposition) p et q.
2. Calculez la clef secrète d.
3. Déchiffrez le cryptogramme.

Exercice 4

Bob choisit comme nombre premier $p = 17$ et $q = 19$, comme exposant $e = 5$. Alice et lui se fixent un protocole RSA dans lequel les messages sont des nombres en base 10 que l'on code par bloc de 2 chiffres. Alice veut envoyer le message "462739".

1. Donnez la clef publique de Bob.
2. Donnez la clef secrète d de Bob.
3. Écrivez le message chiffré que Alice envoie à Bob.
4. Déchiffrez le message qu'a reçu Bob et vérifiez que c'est bien celui qu'a envoyé Alice.

3 Devoir maison

Encore du RSA

Bob utilise le protocole RSA et publie sa clef publique $n = 187$ et $e = 3$.

1. Encodez le message $m = 15$ avec la clef publique de Bob.
2. En utilisant le fait que $\varphi(n) = 160$, retrouvez la factorisation de n.
3. Retrouvez la clef privée d de Bob.

Carré de Polybe

Le chiffrement par la méthode du carré de Polybe consiste à remplacer chaque lettre par une paire de chiffre indiquant sa place dans un tableau. Par exemple dans le tableau 1, la lettre "f" est codée par 21. (Les lettres "i" et "j" sont codées par le même nombre pour permettre un tableau de taille 5x5). On utilise cette méthode pour chiffrer en prenant un ordre de lettres aléatoire dans le tableau, la clef secrète est ainsi donnée par le tableau de chiffrement/déchiffrement.

1. Décoder le message suivant avec le second carré 34 21 34 25 33 52 43 35 51 23 42 45 33 55 13 31 53 33 21 43 52 51 43 13 35 43 33 45 43 32 34 33 13 33 23 31 33 34 33 31 21 34 31 32 33 31 51 12 55 21 34 31 15 43 33 34 33 23 33 31 21 34 31 12 34 33 23
   Qui est l'auteur de cette citation ?
2. Combien existe t'il de clef possible ? Donner une estimation du temps pour une attaque par force brute.
3. A quelle famille de code cette méthode appartient-elle ? Quelle méthode d'attaque est possible ?

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

	1	2	3	4	5
1	x	r	p	y	q
2	a	w	n	k	v
3	s	d	e	i/j	l
4	z	g	u	h	t
5	o	c	b	f	m