TD1 : Chiffrement basique

1 Chiffrement de César

1. Chiffrer le message “la rencontre est prévue à la cafétéria” ‘a l’aide du chiffrement par décalage et de la clé $K = 5$.
2. Décrypter le message “RGNEIDVGPEWXTRAPHHXFJT” sachant qu’il a été créé par un chiffrement par décalage et que le message en clair contient deux occurences de la lettre C.
3. Dans un texte en français les lettres les plus fréquentes sont le A (8.4%) et le E (17.26%). Sachant que le message est en français déterminer la clef et décrypter le message :
SVOXFYIKNKXCVKVSQEBSOKMRODOBNOCCYVNKDC

2 Chiffrement par substitution

1. Chiffrer le message “la rencontre est prévue à la cafétéria” à l’aide du chiffrement par substitution et de la clé suivante :

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

2. Décrypter le message “YHVMQUVMH” sans connaitre la clé est-il possible ? Décryptez le sachant que la clé est la même que celle utilisée au dessus.

3 Chiffrement de Vigenère

Rappel : dans le chiffrement de Vigenère, un décalage par A est un décalage de 0.

1. Chiffrer le message “la rencontre est prévue à la cafétéria” à l’aide du chiffrement de Vigenère et de la clé POULE
2. Décrypter le message “CW MFL CCWF VKT CW NFE D’LFE DWTYGDV VE TZIWXRVEEEL UKALZKEV HOLJ SJZ” en trouvant la clé en sachant qu’elle a une longueur de 3 (Notez que l’on a gardé les espaces et apostrophes pour vous aider).

4 Chiffrement XOR

1. Chiffrer le message “1101 1110 0110 0001 1101 0011 1110 0100” à l'aide du chiffrement XOR et de la clé 10011001.
2. Déchiffrez le message “1101 1110 0110 0001 1101 0011 1110 0100” à l'aide de la même clef.

5 Chiffrement symétrique vs asymétrique

Vous êtes dans un groupe de n personnes (dont Alice et Bob) souhaitant utiliser un système cryptographique. Le but est que la communiquation de pair à pair soit confidentielle, càd que lorsque deux membres du groupes échangent des informations, aucun autre membre du groupe ne puisse décrypter ces messages.

1. Le groupe souhaite utiliser un système de chiffrement symétrique. Proposez en un.
2. Combien de clefs doit-on générer pour tout le groupe afin d'assurer que les communiquations restent confidentielles ?
3. Expliquez pourquoi le groupe devrait utiliser un chiffrement asymétrique, et proposez en un.
4. Le groupe a décidé d'utiliser votre proposition de chiffrement asymétrique. Si Alice envoie à Bob un message crypté et signé, quelle clef Bob doit-il utiliser pour le décrypter ?
5. Combien de pairs clef publique/clé privée doit-on générer pour tout le groupe ?

6 Protocole d'authentification

Supposons que l'on ait un chiffrement asymétrique et que Alice et Bob communiquent sur un canal public. On propose le protocole d'authentification suivant.

— Alice envoie sa clef publique à Bob

— Bob envoie sa clef publique à Alice

— Alice produit un message et le signe avec sa clef privée. Puis elle l'encrypte avec la clef publique de Bob avant de lui envoyer.

— Bob décrypte le message en utilisant sa clef privée, puis vérifie que la clef privée de Alice correspond bien en utilisant la clef publique qu'elle lui a communiquée.

Ce protocole est-il un bon protocole d'identification ? Si oui, pourquoi ? Si non, expliquez pourquoi et comment l'attaquer.

7 Ordre de grandeur

Imaginons un système protégé par un mot de passe. Le système limite l'utilisateur à un essai par seconde. Combien de temps faut-il pour pénétrer le système de manière "brute force" dans ces différents cas :

1. le mot de passe est un prénom
2. le mot de passe est un mot du dictionnaire français
3. le mot de passe est une séquence de 4 chiffres (type code PIN)
4. le mot de passe est composé de 8 caractères alphanumériques (incluant les 15 signes de ponctuation)

(Vous pouvez chercher en ligne pour répondre aux 2 premiers).

8 Chiffrement RSA

On rappelle comment fonctionne RSA basiquement (on prouvera pourquoi il mache au prochain TD) :

— On génère un entier n qui est le produit de 2 nombres premiers p et q.

— On génère un entier e premier avec $(p-1) \times (q-1)$. On note (e, n) la clef publique.

— On trouve un entier d tel que $e \times d = 1 \mod (p-1) \times (q-1)$. On note (d, n) la clef privée.

— On chiffre un message m par $m^e \mod n$, et on déchiffre un message m par $m^d \mod n$.

On prouvera au prochain TD pourquoi $m^{e \times d} = m \mod n$.

1. On rappelle le théorème de Bézout : Pour tout entiers a et b, il existe des entiers relatifs u et v tels que $au + bv = \text{pgcd}(a, b)$.
   Montrez que l'on peut toujours trouver un entier d comme ci-dessus.
2. Chiffrez 21 avec la clef publique $(103, 143)$.
3. Décomposez 143 comme un produit de 2 nombres premiers et calculez la clef privée associée à $(103, 143)$.
4. Déchiffrez le message 13.