TD1

mercredi 16 novembre 2022 10:16

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

1/ Qf wjshtywj jxy uwjazj f qf hfkjyjwnf
2/ Cryptographie classique : K = 15
3/ il envoya dans la … : K = 16

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

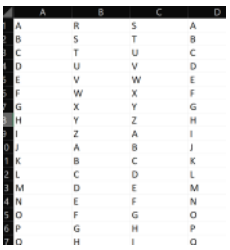
2. Décrypter le message “YHVMQUVMH” sans connaitre la clé est-il possible ? Décryptez le sachant que la clé est la même que celle utilisée au dessus.

1/ BX CHSYFSMCH HVM LCHEUH X BX YXPHMHCZX
2/ C'est juste

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).



1/ ao lprrchevt sme tvtjop p zu ne…
2/ Clé : RSA : le mot cle est le nom d'une methode de chiffrement utilisée pour ssh

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 ?

3/ On ne sait pas si l'autre personne gardera sa clé confidentielle.
Ex : RSA
4/ …