Initiation à la cryptographie

Travaux Dirigés de cryptographie n°1

—TELECOM Nancy 2A ISS—

1 Protocoles

▸ **Exercice 1.** Message confidentiel et authentifié

Alice doit envoyer un message confidentiel et authentifié à Bob, mais ne dispose que d'un canal public. Elle utilise le protocole suivant :

- Bob envoie sa clé publique à Alice.
- Alice envoie sa clé publique à Bob.
- Alice produit son message, le signe avec sa clé privée, et le chiffre avec la clé publique de Bob.
- Bob reçoit le message, le déchiffre avec sa clé privée, et vérifie que la signature colle avec la clé publique d'Alice.

Où est le lézard ?

▸ **Exercice 2.** SSH

Dans le livre *SSH, the secure shell*[1], les auteurs décrivent la phase d'identification d'un client SSH auprès d'un serveur SSH.

La suite d'échanges suivante correspond à la conversation entre un client et un serveur :

(*i*) le client : « Bonjour serveur, je voudrais obtenir une connexion SSH sur un de vos comptes, plus particulièrement sur le compte dénommé SMITH. »

(*ii*) le serveur répond : « Eh bien, pourquoi pas. Je vais tout d'abord vous proposer un défi pour m'assurer de votre identité ! » Le serveur envoie alors des données, correspondant au défi, au client.

(*iii*) le client répond : « J'accepte le défi. Voici la preuve de mon identité. Je l'ai calculée moi-même à partir de votre défi et de ma clé privée. » Cette réponse au serveur est appelée un *authentificateur*.

(*iv*) le serveur répond : « Merci. Je vais maintenant examiner le compte SMITH pour voir si vous pouvez vous connecter. » Plus précisément, le serveur examine les clés publiques de SMITH pour vérifier si l'une d'elle correspond bien à l'authentificateur que le client a donné Si c'est le cas, le serveur répond alors : « OK, vous pouvez accéder à votre compte » ; sinon : « L'authentification a échoué. »

Nous allons identifier les différentes primitives cryptographiques utilisées dans ce programme.

1. Décrivez de manière plus précise les opérations intervenant dans ces différentes phases de l'identification. En particulier, quel(s) type(s) de système(s) cryptographique(s) permet(tent) de réaliser ce protocole ? Montrez avec un exemple le déroulement de ce protocole.
2. Avant qu'une telle connexion entre un client et un serveur SSH ne puisse s'établir, qu'est-il nécessaire de mettre au point au préalable ?
3. Si le protocole n'avait pas précisé clé privée, clé publique, quel autre mécanisme pourriez-vous proposer ? Commentez.

1. de D.J. Barrett & R.E. Silverman, publié chez O'Reilly en 2001

2 Substitutions

▸ **Exercice 3.** Chiffrement par décalage (César)

1. Chiffrer le message “la rencontre est prévue à la cafétéria” à 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.
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, chiffré en utilisant le chiffrement par décalage sur les 26 lettres de l’alphabet, déterminer la clef et décrypter le début du message :
   SVOXFYIKNKXCVKVSQEBSOKMRODOBNOCCYVNKDC

▸ **Exercice 4.** 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. Est-il possible de décrypter le message “YHVMQUVMH” chiffré par un chiffrement par substitution sans connaître la clé ? Déchiffrer ce message sachant qu’il a été créé avec la clé précédente.

▸ **Exercice 5.** Chiffrement de Vigenère

1. Chiffrer le message “la rencontre est prévue à la cafétéria” à l’aide de la méthode de Vigenère et du mot clé POULE.
2. Est-il possible de décrypter le message “BAUNBEKLZLQSKQKEBGCJYHVSKR” chiffré par un chiffrement de Vigenère sans connaître la clé ? Déchiffrer ce message sachant qu’il a été créé à l’aide du mot clé TNCY.

Ici la lettre “A” correspond à un décalage de 0.

3 Se familiariser avec les ordres de grandeur

▸ **Exercice 6.** Mot de passe

Un système est protégé par un mot de passe. Après un essai infructueux le système attend 1 seconde avant de redemander le mot de passe. Combien de temps faudra-t-il pour pénétrer le système dans les cas suivants :

1. le mot de passe est un prénom ;
2. c’est un mot du dictionnaire ;
3. il est composé de 4 chiffres ;
4. il fait 8 caractères alphanumériques (y compris les 15 signes de ponctuations)

▸ **Exercice 7.** La force brute

Le *facteur de travail* d'un algorithme est le nombre d'instructions élémentaires nécessaire à son exécution. La puissance d'une machine est le nombre d'instructions qu'elle exécute par unité de temps. Nous allons approcher la puissance d'un PC actuel à environ 2000 Mips (millions d'instructions par seconde).

Le facteur de travail d'un algorithme optimisé pour tester une clé de 128 bits de l'algorithme AES est d'environ 1200 instructions élémentaires.

On dispose d'un couple clair/chiffré connu et on désire retrouver la clé utilisée par force brute, c'est-à-dire en testant toutes les clés les unes après les autres. Une clé est constituée d'un mot de 128 bits. On suppose que toutes les clés sont équiprobables.

1. En combien de temps une machine de 2000 Mips teste-t-elle une clé ?
2. Combien y a-t-il de clés possibles ? Quel est le nombre moyen de clés à tester avant de trouver la bonne ?
3. À quel temps moyen de calcul cela correspond-il si on suppose qu'un seul PC effectue la recherche ? Si les 1 milliard de PC de l'Internet sont mobilisés à cette tâche ?