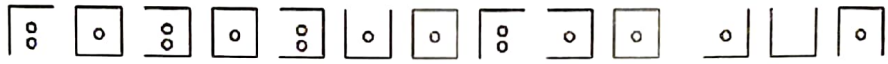
Introduction à la sécurité
L3 Informatique

Examen – 21 Avril 2021 - 2h

Les documents de cours sont autorisés (notes de cours manuscrites ou dactylographiées, sujets de TD/TP et leurs corrections). Les téléphones doivent être éteints. Les ouvrages ou documents externes (livres) sont interdits.
Le barême n'est donné qu'à titre indicatif et pourra être légèrement modifié.

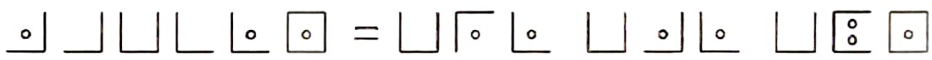
Exercice 1 - Chiffrement de Churchyard (4 points)

Histoire : Ce message chiffré est gravé sur une tombe dans le cimetière de Trinity Churchyard (New York) depuis 1794. Of course le texte chiffré est écrit en anglais. Il fut déchiffré en 1896.



1. (2 points) En utilisant l'astuce, retrouvez le message original ?

ASTUCE = TIC TAC TOE



2. (2 points) Comment fonctionne ce chiffrement ?

Exercice 2 - Etude du jeu de pile ou face en réseau (9 points)

Alice et Bob communiquent à distance au moyen d'un réseau de messages asynchrones. Ayant un différend sur une décision à prendre, ils veulent s'en remettre au hasard pour la décision finale. Pour cela, ils décident de construire un protocole par échange de messages asynchrones qui réalise une décision aléatoire de même nature que celle de pile ou face lorsque deux personnes sont en présence.

La décision à pile ou face comporte traditionnellement le choix au hasard par l'un des participants du coté pile ou face d'une pièce de monnaie et le lancer de la pièce par l'autre participant. Pour remplacer le lancer de la pièce de monnaie Alice et Bob décident de tirer un entier au hasard n non nul. Selon que l'entier n est pair ou impair, on considère que la pièce est retombée coté pile ou coté face. Pour remplacer le choix au hasard entre pair et impair, Alice et Bob décident d'utiliser le tirage aléatoire d'une variable binaire p.

Alice et Bob se méfient l'un de l'autre et souhaitent déterminer un protocole ayant un bon niveau de sécurité c'est-à-dire que l'un comme l'autre ne doit pas pouvoir tricher et doit pouvoir vérifier que l'autre ne triche pas.

Le protocole à définir n'utilisera pas de tiers de confiance qui assurerait pendant le déroulement un rôle d'arbitrage. Une version de base du protocole pourrait être la suivante :

Alice		**Bob**
Choisit n au hasard		Choisit le bit p au hasard
Envoie n en clair	$\xrightarrow{n}$	
	$\xleftarrow{p}$	Envoie p en clair
	Décision Finale	
Alice gagne si Bob n'a pas donné la bonne parité		Bob gagne si il a donné la bonne parité

1. Etudiez le protocole précédent. Quelles sont les fraudes possibles de la part de Alice ou Bob ?

Pour garantir la sécurité de la décision finale, Alice et Bob étudient la possibilité d'utiliser des fonctions cryptographiques. Ils souhaitent tout d'abord construire une solution qui utilise un chiffrement symétrique comme l'AES par exemple. On note E_K ce chiffrement paramêtré par une clé secrète K. Le protocole utilisé devient alors :

Alice		**Bob**
Choisit n au hasard		Choisit le bit p au hasard
Choisit la clé secrète K		
Envoie $E_K(n)$	$\xrightarrow{E_K(n)}$	
	$\xleftarrow{p}$	Envoie p en clair
Envoie K et n en clair	$\xrightarrow{K,n}$	
	Décision Finale	
Alice gagne si Bob n'a pas donné la bonne parité		Bob gagne si il a donné la bonne parité

2. Etudiez le protocole précédent. Quelles sont les fraudes possibles de la part de Alice ou Bob ? Justifier votre réponse.

Comme le protocole précédent ne semble toujours pas sûr, Alice et Bob décident d'utiliser un algorithme de chiffrement à clé publique, plus précisement RSA.

3. Faite un dessin du nouveau protocole en considérant que c'est Alice qui choisit la paire de clés RSA ($Kp_A = (e, N), Ks_A = (d)$) et qui révèle d à la dernière étape du protocole avant la décision finale.

En fait, cette nouvelle version n'est toujours pas sûre car Alice peut chercher un nombre s qui est tel que $s \bmod N = n^e \bmod N$ et duper encore Bob.

Cette fois-ci, Alice et Bob décident d'utiliser une fonction de hachage cryptographique H et le protocole suivant :

Alice		Bob
Choisit n au hasard		Choisit le bit p au hasard
Envoie $H(n)$	$\xrightarrow{H(n)}$	
	$\xleftarrow{p}$	Envoie p en clair
Envoie n en clair	$\xrightarrow{n}$	
	Décision Finale	
Alice gagne si Bob n'a pas donné la bonne parité		Bob gagne si il a donné la bonne parité

4. Rappelez la définition d'une fonction de hachage et les propriétés que doit vérifier cette fonction de hachage pour être qualifiée de cryptographique.

5. En supposant que la fonction de hachage utilisée H est cryptographique, que pensez-vous à présent du protocole ? Justifier votre réponse.

6. Après toutes ces versions, la dernière version semble la meilleure ! Quelle propriété du canal voulait-on en fait garantir ?

7. Alice et Bob souhaitent à présent définir un protocole qui puisse être, en cas de litige, soumis à un juge. Pour cela, Alice et Bob se proposent de modifier le protocole avec fonction de hachage et d'ajouter l'utilisation d'autres fonctions cryptographiques. Comme la propriété cryptographique que l'on souhaite garantir est la non-répudiation, quelle fonction cryptographique faut-il ajouter ? Justifiez les mécanismes introduits permettant de défendre le point de vue que seuls Alice ou Bob peuvent être l'auteur de leurs messages. Dessinez le nouveau protocole.

Exercice 3 - Crypto Symétrique et Asymétrique (3 points)

Un groupe de n personnes souhaite s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres ne doivent pas pouvoir être lues par les autres.

1. Dans le cas où le groupe choisit un système de chiffrement symétrique, quel est le nombre minimal de clefs nécessaires ?
2. Dans le cas où le groupe choisit un système de chiffrement asymétrique, quel-est le nombre minimal de couples de clefs nécessaires ?
3. Synthétiser sous forme d'un tableau les avantages et inconvénients respectifs du chiffrement symétrique et asymétrique. Le groupe choisit finalement un système hybride qui utilise la cryptographie symétrique et asymétrique comme PGP, pourquoi ?

Exercice 4 - Diffie-Hellman (4 points)

Le protocole d'échange de clés Diffie-Hellman fonctionne sur le problème du logarithme discret de la manière suivante :

- Alice et Bob veulent construire une clé commune K.
- Pour cela, Alice choisit p un grand nombre premier, et g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Elle les rend publics.
- Alice choisit a et le garde secret et envoie à Bob $A = g^a \mod p$.
- Bob choisit b et le garde secret et envoie à Alice $B = g^b \mod p$.
- Le secret commun est alors $K = g^{ab} \mod p = A^b \mod p = B^a \mod p$ que à la fois Alice et Bob peuvent calculer.

1. Quel est le secret commun qu'établissent Alice et Bob en utilisant le protocole de Diffie-Hellman avec $p = 11$ et $g = 2$ si les nombres aléatoires qu'ils ont choisis sont $a = 5$ et $b = 6$?
2. Le protocole de Diffie-Hellman ne peut être utilisé en l'état car il existe contre celui-ci une attaque appelée "attaque de l'homme du milieu". Pouvez-vous construire cette attaque ? La décrire.