Examen du 24 mai 2005

Durée 3 heures - documents autorisés
Toute réponse devra être justifiée

Exercice 1 : [20min] *Cyber-contribuables ...*

Voici un certificat utilisé dans le cadre de la déclaration en ligne de revenus 2004 :

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            46:8c:74:45:5f:a8:51:ad:ec:8c:28:a4:6b:34:8c:dd
        Signature Algorithm: md5WithRSAEncryption
        Issuer: O=DIRECTION GENERALE DES IMPOTS, CN=AC DIRECTION GENERALE DES IMPOTS USAGER
        Validity
            Not Before: Mar 24 00:00:00 2005 GMT
            Not After : Mar 23 23:59:59 2008 GMT
        Subject: C=fr, O=DIRECTION GENERALE DES IMPOTS,
                 OU=DIRECTION GENERALE DES IMPOTS USAGER, OU=AD - 1, OU=D - 2,
                 CN=XXXXXXXXXXXXXX/emailAddress=xxxxx@xxxxxx.xx
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00:b5:b1:4f:6d:25:9d:b6:7c:fd:51:87:af:f8:76:
                    60:dd:f5:3e:3e:c2:2a:89:fe:91:fa:4c:22:37:26:
                    0a:19:c3:ed:43:72:80:76:9e:de:ac:cb:fc:08:35:
                    49:b5:00:b0:8a:7d:1c:42:33:38:7b:89:04:86:7d:
                    89:3b:38:bd:e7
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 CRL Distribution Points:
                URI:http://onsitecrl.certplus.com/DIRECTIONGENERALEDESIMPOTS ...

            X509v3 Key Usage:
                Digital Signature, Non Repudiation
            Netscape Cert Type:
                SSL Client
            2.16.840.1.113733.1.6.9:
                ...
    Signature Algorithm: md5WithRSAEncryption
        48:d8:7f:ce:3f:c6:f8:6d:64:b6:b1:70:09:2e:3d:0d:04:71:
        91:57:86:01:ea:56:67:8e:95:6d:b9:8d:19:e9:ad:4f:e1:1b:
        8c:b6:71:ba:ea:93:b6:7b:99:7a:a4:d1:7f:40:07:a2:5b:c2:
        3a:21:64:22:64:81:e4:0a:71:98:10:bf:da:54:07:6e:fb:8d:
        af:7e:9f:3e:53:45:e0:ee:fa:ec:0e:92:29:0e:76:55:59:79:
        26:13:5a:4b:8b:9d:89:c4:ca:7f:bb:50:17:25:13:e1:ef:11:
        2a:e5:0a:e2:c1:ef:73:08:3c:a6:56:4e:5b:e7:2f:69:7e:26:
        78:c9
```

Q 1 . Qui a délivré ce certificat ?

Q 3 . Pouvez-vous citer deux usages de ce certificat ?
Q 4 . Expliquez le choix de l'exposant public ?
Q 5 . En vous appuyant sur l'expertise que vous avez acquise cette année dans le cours de PAC, et au vu de ce certificat, avez-vous des remarques à formuler à propos de la sécurité du service de déclaration en ligne des revenus 2004 ?

Exercice 2 : [15min] *Télécommunications*

En télécommunications, l'information doit être protégée

- contre les bruits ambiants en utilisant des codes correcteurs, qui rallongent le message on lui apportant de la redondance, permettant ainsi de détecter et corriger les incohérences liées aux erreurs de transmissions,
- contre les indiscrétions en utilisant des systèmes de chiffrement.

Q 1 . Pour protéger un message m de ces deux menaces, on peut le transformer successivement de deux façons :

1. on le chiffre avant de lui appliquer un code correcteur d'erreurs ;
2. on lui applique un code correcteur d'erreurs avant de le chiffrer.

Discutez ces deux solutions.

Exercice 3 : [10min] *Alice et Bob*

Voici un échange de courrier entre Alice et Bob.
Le courrier de Bob

> Ma chère Alice,
>
> Voici un message que j'ai chiffré (je ne te dis pas comment) :
>
> `HTFR8THN/NX/A?ZD1PIQN/1 KNGSNFSHQSOYRQTA?D G GFH ETRQZDFD// QQDFG .DFG QG QF1 GHINEQERQZV FLYPRDTPVY BDUKOYPNIOPTP TSRTNRV/`
>
> Arriveras-tu à le décrypter ?

La réponse d'Alice

> Mon cher Bob,
>
> J'ai décrypté ton message : c'est le début du "traité pour une constitution européenne" pour lequel nous sommes appelés à voter ce dimanche, chiffré avec du one-time pad.
>
> N'ai-je pas raison ?

Q 1 . Alice a-t-elle raison ? Discutez !

Exercice 4 : [30min] *LFSRs*

On considère le LFSR donné en figure 1.

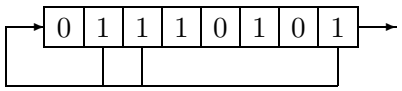

Figure 1: Le LFSR

Q 1 . Quel est son polynôme de rétroaction ?
Q 2 . Ce polynôme est-il irréductible dans $\mathbb{F}_2$? Est-il primitif ? Qu'en concluez-vous ?
Q 3 . Déterminez la complexité linéaire de la suite produite par ce LFSR, et donnez le plus petit LFSR qui la génère.
Q 4 . Considérons maintenant le LFSR que vous venez d'obtenir à la question précédente. Que peut-on dire de la suite qu'il produit si on l'initialise avec un autre état ?

Voici 8 parts d'un secret partagé avec le schéma à seuil de Shamir. Le seuil est $t = 3$ et le nombre premier est $p = 59$.

Part numéro 1	27	Part numéro 2	26
Part numéro 3	24	Part numéro 4	21
Part numéro 5	17	Part numéro 6	11
Part numéro 7	6	Part numéro 8	58

Table 1: Les 8 parts d'un secret partagé

Q 1 . Retrouvez le secret à partir des parts numéros 1, 2 et 3.
Q 2 . Parmi les autres parts l'une est incorrecte. Laquelle ?
Q 3 . On s'intéresse au problème de la détection d'une part introduite par un participant malhonnête dans un schéma de partage de secret à seuil de Shamir, ce participant introduisant une part choisie au hasard. À partir de combien de parts réunies, et avec quelle probabilité les participants peuvent-ils détecter cette intrusion ?

Exercice 6 : [25min] *Confidentialité parfaite*

Considérons le système de chiffrement symétrique défini par

1. l'ensemble des messages clairs : $\mathcal{P} = \{1, 2, 3\}$,
2. l'ensemble des chiffrés : $\mathcal{C} = \{a, b, c, d, e, f\}$,
3. l'ensemble des clés : $\mathcal{K} = \{k_1, k_2, k_3, k_4, k_5, k_6\}$,

et la fonction de chiffrement $E(m, k)$ décrite par le tableau suivant :

m	1	2	3
$E(m, k_1)$	a	b	c
$E(m, k_2)$	c	a	b
$E(m, k_3)$	b	c	a
$E(m, k_4)$	d	e	f
$E(m, k_5)$	f	d	e
$E(m, k_6)$	e	f	d

Q 1 . Pour quelle distribution de probabilités sur $\mathcal{K}$ ce système est-il à confidentialité parfaite ?

Exercice 7 : [1h] *Fonction de hachage de Chaum - van Heijst - Pfitzmann*

Soit p un (grand) nombre premier impair tel que $q = \frac{p-1}{2}$ est aussi premier. Soient α et β deux éléments primitifs de $(\mathbb{Z}/p\mathbb{Z})^*$. (rappel : un élément α est primitif modulo p si le plus petit exposant $m > 0$ tel que $\alpha^m = 1 \pmod p$ est $m = p - 1$)

La fonction de hachage de Chaum - van Heijst - Pfitzmann est définie par

$$\begin{array}{rccl} h & : & \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ & & x_1, x_2 & \mapsto & h(x_1, x_2) = \alpha^{x_1}\beta^{x_2} \mod p \end{array}$$

Q 1 . On prend $p = 83$, $q = 41$, $\alpha = 2$ et $\beta = 6$.

Q 1.1. Vérifiez que α et β sont deux éléments primitifs de $(\mathbb{Z}/83\mathbb{Z})^*$. Indiquez les calculs que vous effectuez.

Q 1.2. Avec ces paramètres, calculez $h(50, 48)$.

Q 2 . Exprimez le coût algorithmique du calcul de $h(x_1, x_2)$ en fonction de la taille de p.

Q 3 . Cette fonction est prouvée être à préimage, collisions faibles et collisions fortes difficile sous l'hypothèse de la difficulté d'un certain problème mathématique. Quel est ce problème ?

Q 4 . Cette fonction transforme un couple d'entiers modulo q en un entier modulo p. Elle hache donc un "document" de taille $2n - 2$ bits en une empreinte de n bits.

Indiquez comment utiliser cette fonction pour hacher des documents de toute taille tout en préservant les bonnes propriétés de h.

Estimez la quantité de calcul.

Q 5 . Les fonctions de hachage sont utiles en signature ; discutez l'intérêt d'utiliser la fonction de hachage de Chaum *et al.* dans ce contexte.