heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Cryptographie

Examen Final

2 février 2018

Nom :

Prénom :

- N'oubliez pas d'inscrire votre nom sur *chacune* des pages impaires de l'examen !
- Durée du travail écrit : 120 minutes
- Matériel autorisé : 1 page A4 (recto-verso) de résumé personnel, du matériel pour écrire et une calculatrice non-programmable.
- Le total de points de cet examen est de **88 points**.
- Cet examen comporte 18 pages.

Interdiction de tourner cette page avant le début de l'examen !

Page vide

Nom : Prénom :

1 SSL/TLS (10 pts)

1. Vous vous connectez pour la première fois sur le site web `www.debian.org` à l'aide de TLS. La ciphersuite choisie est `TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256`.
   Expliquez comment une connexion sécurisée et authentifiée est obtenue. Indiquez le plus précisément possible qui possède quelle clef et quels algorithmes sont utilisés. **(5 pts)**

2. Lors d'une connexion HTTPS (bien configurée), qu'est-ce qui empêche les attaques de type "homme du milieu" (man-in-the-middle) ? **(1 pts)**

3. Un site marchand décide de créer sa propre app pour smartphone afin de gérer les achats de ses clients. Cette app se connecte au serveur du site marchand, vérifie le certificat du serveur et effectue ensuite les transactions. Malheureusement, lors de la vérification du certificat, l'app oublie de vérifier que le sujet du certificat correspond bien au serveur du site marchand.
   Expliquez comment un attaquant peut lire les données transitant entre l'app et le serveur. **(4 pts)**

Nom : Prénom :

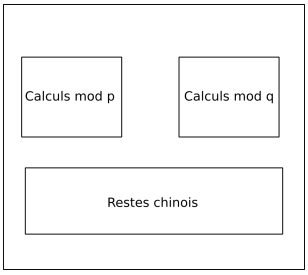
2 Fault Attack sur les Signatures RSA (12 pts)

Une smartcard est utilisée pour effectuer des signatures RSA. Elle utilise les signatures de type "textbook" RSA. Les signatures sont accélérées à l'aide du **théorème des restes chinois**. Les exponentiations sont effectuées à l'aide de l'algorithme **square-and-multiply**.

1. Soit p et q les nombres premiers utilisés pour RSA. Soit $N = pq$. Soit (e, N) la clef publique et (d, N) la clef privée. Expliquez comment on peut accélérer la signature à l'aide du théorème des restes chinois. **(3 pts)**

2. Si $p = 5$, $q = 7$ et $d = 5$. Que vaut la clef publique ? Que vaut la signature "textbook" RSA du message $m = 10$? Donnez les étapes de calcul dans le cas où le **théorème des restes chinois** est utilisé. **(3 pts)**

3. La puce de la smartcard suit le design suivant :



La clef privée est stockée dans la smartcard et vous souhaitez la récupérer. A l'aide d'un laser, vous pouvez chauffer une portion de la smartcard afin qu'elle fasse des erreurs de calcul. Vous savez aussi que

$$2^{511} \leq p < 2^{511} + 2^{509}$$
$$2^{511} + 2^{510} \leq q < 2^{512}$$

Vous avez le droit de demander à la smartcard d'effectuer une seule signature. Expliquez comment récupérer la clef privée. **(5 pts)**

4. L'attaque précédente est-elle de type blackbox, greybox ou whitebox ? Justifiez. **(1 pt)**

Nom : Prénom :

3 Chiffrement d'El Gamal (15 pts)

Pour le chiffrement d'El Gamal, on a pour paramètres un élément g d'ordre q dans $\mathbb{Z}_p^*$, avec p et q premier.
Clefs : La clef privée est un $b \in \mathbb{Z}_q$. La clef publique : $y_b = g^b \bmod p$.
Chiffrement d'un message M :
— On tire un $a \in \mathbb{Z}_q$ au hasard.
— Le chiffré est la pair $(g^a \bmod p, M(y_b)^a \bmod p)$.
Déchiffrement d'une paire (s,t) : calculer $ts^{-b} \bmod p$.

1. Expliquez comment générer efficacement p et q de telle sorte qu'il soit possible d'avoir un élément g d'ordre q dans $\mathbb{Z}_p^*$. **(3 pts)**

2. On a $p = 19$. Quel est l'ordre de $g = 7$ dans $\mathbb{Z}_p^*$? **(3 pts)**

3. On a $p = 123\,001$ et $g = 17\,036$. L'ordre de g est 41. Que vaut $g^{206} \bmod p$? **(3 pts)**

4. Montrez que pour un chiffré valide, le déchiffrement fonctionne (il retourne le bon texte clair). **(2 pts)**

5. Comme pour RSA, le chiffrement d'El Gamal est malléable. Montrez comment, à l'aide de deux textes chiffrés, on peut obtenir un texte chiffré correspondant au produit des deux messages clairs. Plus précisément, Soit c_1 le texte chiffré correspondant au message M_1 et c_2 le texte chiffré correspondant au message M_2, donnez un texte chiffré c_3 correspondant au message $M_1 \cdot M_2$.
   Note : vous ne connaissez ni M_1, ni M_2. **(4 pts)**

Nom : Prénom :

4 ECDH (14 pts)

On rappelle la formule d'addition de points sur une courbe elliptique sur $\mathsf{GF}(p)$:
— Soient deux points $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ sur une courbe elliptique avec $x_1 \neq x_2$.
— $R = (x_3, y_3) = P + Q$ possède les coordonnées

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 &= -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) \end{aligned}$$

On rappelle la formule de doublement de points :
— Soit un point $P = (x_1, y_1)$ sur une courbe elliptique.
— $R = (x_2, y_2) = 2P$ possède les coordonnées

$$\begin{aligned} x_2 &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_2 &= \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_2) - y_1 \end{aligned}$$

Dans ce problème, on considère la courbe elliptique E définie par l'équation $y^2 = x^3 + 5x + 3$ sur $\mathsf{GF}(7)$.

1. Quels sont les points sur la courbe elliptique E ? **(3 pts)**

2. Sur E, que vaut $(6,2)+(6,5)$? **(2 pts)**

3. On utilise E pour effectuer le protocole ECDH (elliptic curve Diffie-Hellman). Pour ceci, on utilise le point $G=(6,2)$. Alice tire comme paramètre privé $a=3$. Quelle valeur Y_a est envoyée à Bob par Alice lors de l'exécution du protocole ? **(4 pts)**

Nom : Prénom :

4. Dessinez le protocole ECDH entre Alice et Bob. **(2 pts)**

5. Lors du protocole ECDH, quelle attaque peut effectuer un adversaire actif ? Détaillez. **(3 pts)**

5 CBC-MAC (8 pts)

1. Expliquez comment fonctionne CBC-MAC. A quoi faut-il faire attention ? Quelle alternative pouvez-vous proposer ? **(4 pts)**

2. Etant donné un message m composé d'au moins deux blocs et son MAC (dénommé τ), montrez comment un attaquant peut forger facilement un MAC valide pour un nouveau message m'.
   Indice : Ajoutez des blocs à la fin de m pour obtenir m'. **(4 pts)**

Nom : Prénom :

6 PRNG (9 pts)

Dans ce problème, nous allons nous intéresser à différents générateurs de nombres premiers de 512 bits. Ces nombres premiers seront ensuite utilisés **pour générer des clefs RSA**. Pour chaque question, commentez

— sa sécurité.

— son efficacité.

1. Soit H une fonction de hachage (sûre) avec une sortie de 512 bits. On tire un nombre aléatoire n entre 1 et 100 000, on calcule $H(n)$ et on teste si le résultat est premier. Si ce n'est pas le cas, on recommence avec un autre n. **(2 pts)**

2. On tire 512 pièces de monnaie. [1] Chaque pile correspond à un bit 0 et chaque face à un bit 1. On utilise ensuite le crible d'Erathostène pour tester si le résultat est premier. Si ce n'est pas le cas, on recommence. **(2 pts)**

1. On suppose qu'on a une méthode efficace pour tirer rapidement des pièces de monnaie.

3. Soit H une fonction de hachage (sûre) avec une sortie de 512 bits. On prend la date du jour au format `yyyymmdd` et on la convertit en entier n. On incrémente n jusqu'à ce que $H(n)$ soit premier. **(2 pts)**

4. Comment génèreriez-vous un nombre premier de 512 bits ? Expliquez comment vous obtenez un nombre aléatoire et comment vous testez s'il est premier. Il n'est pas nécessaire d'aller dans les détails des algorithmes. **(3 pts)**

Nom : Prénom :

7 Choix de Primitives (12 pts)

Un ami est au courant de vos grandes compétences en cryptographie et veut vous demander conseil. Pour chacun des scénarios suivants, indiquez une solution cryptographique résolvant son problème.

1. Une entreprise souhaite vendre du matériel informatique depuis son site web. Ayant lu quelques articles de journaux, elle a peur que ses clients se fassent voler leur numéro de carte de crédit durant la transaction. **(3 pts)**

2. Deux serveurs d'une même entreprise souhaitent s'échanger un grand volume d'information. Il est important que ces informations restent confidentielles et qu'elle ne puissent pas être modifiées. **(3 pts)**

3. Votre ami souhaite envoyer des emails à ses clients et souhaite qu'ils aient un moyen de vérifier que ces emails proviennent bien de lui. **(3 pts)**

4. Alice et Bob habitent à 10'000 km de distance et souhaitent communiquer de façon sécurisée. Ils ne se sont pas échangé de clefs et ne peuvent pas se rencontrer dans un futur proche. **(3 pts)**

Nom : Prénom :

8 Misc (8 pts)

1. Que vaut $\varphi(252)$? **(4 pts)**

2. Quel est l'inverse de 20 modulo 43 ? **(4 pts)**

3. Quels étaient les noms des trois polonais ayant cryptanalysé Enigma en premier ? **(0 pts)**

Page vide