Utilisation de signatures numériques

Objectifs

Comprendre le principe des signatures numériques.

Partie 1 : Montrer comment utiliser les signatures numériques.

Partie 2 : Montrer comment vérifier les signatures numériques.

Contexte/Scénario

Une signature numérique est une technique mathématique utilisée pour valider l'authenticité et l'intégrité d'un message numérique. Une signature numérique est l'équivalent d'une signature manuscrite. En réalité, les signatures numériques sont bien plus sécurisées. Le rôle d'une signature numérique consiste à se prémunir contre toute intrusion ou toute usurpation d'identité dans les communications numériques. Dans de nombreux pays, comme aux États-Unis, les signatures numériques ont le même poids juridique que les signatures traditionnellement apposées aux documents papier. Il arrive même que le gouvernement américain publie des versions électroniques de ses budgets, lois et projets de loi dotées de signatures numériques.

Ressources requises

- Ordinateur personnel ou terminal mobile avec accès Internet

Partie 1 : Utilisation des signatures numériques

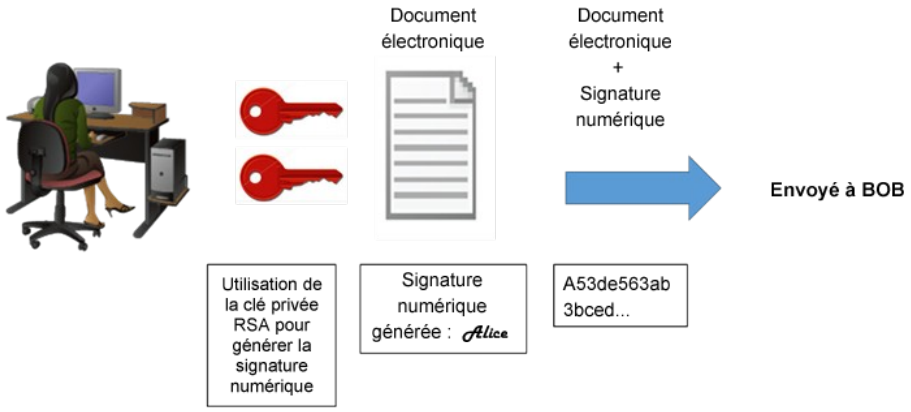
Dans cette partie, vous utiliserez un site web pour vérifier une signature de document entre Alice et Bob. Alice et Bob partagent une paire de clés RSA (clé publique et clé privée). Chacun utilise sa clé privée pour signer un document juridique. Ils s'envoient ensuite les documents l'un à l'autre. Alice et Bob peuvent tous deux vérifier leurs signatures réciproques à l'aide de la clé publique. Ils doivent également convenir d'un exposant de chiffrement public partagé (un nombre premier public partagé) pour effectuer les calculs nécessaires.

Tableau 1 – Clés RSA publiques et privées

Clé RSA publique	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549
Clé RSA privée	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1
Exposant public	10001

Étape 1 : Signez le document.

Alice signe le document juridique, puis l'envoie à Bob à l'aide de la clé publique et de la clé privée RSA du tableau ci-dessus. Bob doit alors vérifier la signature numérique d'Alice afin de s'assurer de l'authenticité du document numérique.



Étape 2 : Vérifiez la signature numérique.

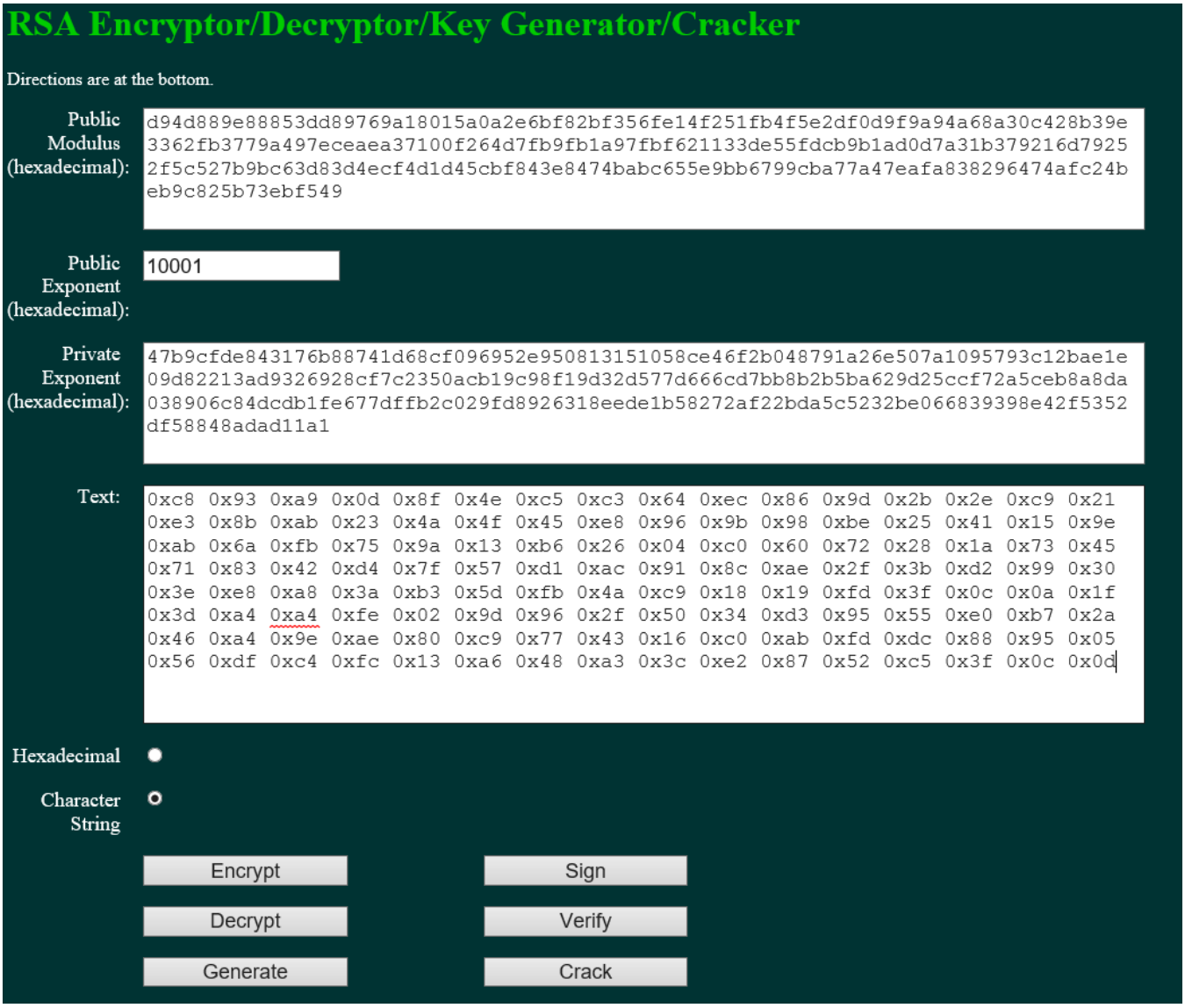
Bob reçoit le document avec la signature numérique du tableau ci-dessous.

Tableau 2 – Signature numérique d'Alice

Signature numérique d'Alice
0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21 0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e 0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45 0x71 0x83 0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30 0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f 0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a 0x46 0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05 0x56 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d

Ouvrez le lien suivant http://nmichaels.org/rsa.py pour utiliser l'outil RSA en ligne et vérifier l'authenticité de la signature numérique d'Alice.

Tableau 3 – Outil en ligne de signature numérique



a. Copiez et collez les clés **publique** et **privée** du Tableau 1 ci-dessus dans les cases **Module public** et **Exposant privé** sur le site web, comme illustré ci-dessus.

b. Assurez-vous que l'exposant public est 10 001.

c. Collez la signature numérique d'Alice copiée sur le tableau 2 dans le champ de texte du site web en suivant l'exemple ci-dessus.

d. Bob peut alors vérifier la signature numérique en cliquant sur le bouton **Vérifier** au milieu du bas de la page du site web. À qui appartient la signature identifiée ?

Étape 3 : Générez une signature de réponse.

Bob reçoit et vérifie le document électronique d'Alice accompagné de sa signature numérique. Il crée alors un document électronique et génère sa propre signature numérique à l'aide de la clé RSA privée du tableau 1 (Remarque : le nom de Bob est en majuscules).

Tableau 4 – Signature numérique de BOB

Signature numérique de BOB
0x6c 0x99 0xd6 0xa8 0x42 0x53 0xee 0xb5 0x2d 0x7f 0x0b 0x27 0x17 0xf1 0x1b 0x62 0x92 0x7f 0x92 0x6d 0x42 0xbd 0xc6 0xd5 0x3e 0x5c 0xe9 0xb5 0xd2 0x96 0xad 0x22 0x5d 0x18 0x64 0xf3 0x89 0x52 0x08 0x62 0xe2 0xa2 0x91 0x47 0x94 0xe8 0x75 0xce 0x02 0xf8 0xe9 0xf8 0x49 0x72 0x20 0x12 0xe2 0xac 0x99 0x25 0x9a 0x27 0xe0 0x99 0x38 0x54 0x54 0x93 0x06 0x97 0x71 0x69 0xb1 0xb6 0x24 0xed 0x1c 0x89 0x62 0x3d 0xd2 0xdf 0xda 0x7a 0x0b 0xd3 0x36 0x37 0xa3 0xcb 0x32 0xbb 0x1d 0x5e 0x13 0xbc 0xca 0x78 0x3e 0xe6 0xfc 0x5a 0x81 0x66 0x4e 0xa0 0x66 0xce 0xb3 0x1b 0x93 0x32 0x2c 0x91 0x4c 0x58 0xbf 0xff 0xd8 0x97 0x2f 0xa8 0x57 0xd7 0x49 0x93 0xb1 0x62

Bob envoie le document électronique et la signature numérique à Alice.

Étape 4 : Vérifiez la signature numérique.

a. Copiez et collez les clés **publique** et **privée** du Tableau 1 ci-dessus dans les cases **Module public** et **Exposant privé** sur le site web, comme illustré ci-dessus.

b. Assurez-vous que l'exposant public est 10 001.

c. Collez la signature numérique de Bob copiée sur le tableau 4 dans le champ de texte du site web en suivant l'exemple ci-dessus.

d. Alice peut alors vérifier la signature numérique en cliquant sur le bouton **Vérifier** au milieu du bas de la page du site web. À qui appartient la signature identifiée ?

Partie 2 : Créez votre propre signature numérique

Maintenant que vous avez vu comment fonctionnent les signatures numériques, vous pouvez créer la vôtre.

Étape 1 : Générez une nouvelle paire de clés RSA.

Accédez au site web de l'outil, puis générez une nouvelle paire de clés RSA (clé publique et clé privée).

a. Effacez le contenu des champs **Module public**, **Module privé** et **Texte**. Utilisez simplement votre souris pour surligner le texte, puis appuyez sur la touche « supprimer » ou Suppr de votre clavier.

b. Assurez-vous que le champ « Exposant public » contient la valeur **10 001**.

c. Générez un nouveau jeu de clés RSA en cliquant sur le bouton **Générer** au milieu du bas de la page du site web.

d. Copiez les nouvelles clés dans le tableau 5.

Tableau 5 – Nouvelles clés RSA

Clé publique	
Clé privée	

e. Saisissez votre nom complet dans le champ **Texte**, puis cliquez sur **Signer**.

Tableau 6 – Signature numérique personnelle

Signature numérique personnelle	

Partie 3 : Échange et vérification des signatures numériques

Vous pouvez désormais utiliser cette signature numérique.

Étape 1 : Échangez vos nouvelles clés, publique et privée, du tableau 5 avec votre partenaire de TP.

a. Notez les clés RSA, publique et privée, du tableau 5 de votre partenaire de TP.

b. Notez les deux clés dans le tableau ci-dessous.

Tableau 7 – Clés RSA de votre partenaire de TP

Clé publique	
Clé privée	

c. Récupérez alors la signature numérique de leur tableau 6. Notez cette signature numérique dans le tableau ci-dessous.

Signature numérique de votre partenaire de TP	

Étape 2 : Vérifiez la signature numérique de votre partenaire de TP.

a. Pour vérifier la signature numérique de votre partenaire de TP, collez ses clés, publique et privée, dans les champs correspondants intitulés **Module public et privé** sur le site web.

b. Collez la signature numérique dans le champ **Texte**.

c. Vérifiez alors sa signature numérique en cliquant sur le bouton Vérifier.

d. Quel texte s'affiche dans le champ de texte ?