TD 3 : Les cryptosystèmes à clé publique Sécurité. Attaques

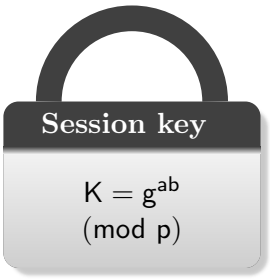
• Echange de clé Diffie-Hellman-Merkle

Exercice 1 Soit un premier p et $\mathbb{Z}_{\mathsf{p}}^{\star} = \langle \mathsf{g} \rangle$ un groupe multiplicatif cyclique.
Choisissez un/une camarade avec qui vous allez communiquer.

1. Choisissez ensemble les paramètres du protocole : p et un générateur g.
2. Sans communiquer, choisissez chacun un nombre secret a, réspectivement b et calculez $\mathsf{A} = \mathsf{g}^{\mathsf{a}} \pmod{\mathsf{p}}$, réspectivement $\mathsf{B} = \mathsf{g}^{\mathsf{b}} \pmod{\mathsf{p}}$.
3. Envoyez à votre camarade votre A (ou B).
4. Il/Elle vous communiquera sa clé partielle B (ou A), mais pas son sécret b (ou a).
5. Calculez $\mathsf{B}^{\mathsf{a}} \pmod{\mathsf{p}}$ (et votre camarade calculera simultanément $\mathsf{A}^{\mathsf{b}} \pmod{\mathsf{p}}$).

• Constatez que vous obtenez le meme nombre. Ce nombre est la clé de session $\mathsf{K} = \mathsf{g}^{\mathsf{ab}}$.

• Remarquez que si quelqu'un avait intercepté vos échanges et avait capté les clés intermédiaires A et B, il aurait été très difficile pour lui de deviner a, b ou la clé de session.



• Protocole El Gamal

Génération des clés

Exercice 2 On considère des nombres premiers à minimum 7 bits, soit supérieurs à $2^7 = 128$.*

1. Choisissez un premier p et $\mathsf{g} \in \mathbb{Z}_{\mathsf{p}}$ un élément d'ordre $\mathsf{q} | (\mathsf{p} - 1)$.
2. Choisissez une clé secrète $\mathsf{sk} = \mathsf{x}$.
3. Calculez votre clé publique $\mathsf{y} = \mathsf{g}^{\mathsf{x}}$.
4. Remarquez que c'est innutile de prendre $\mathsf{x} > \mathsf{q} = \mathsf{ord}(\mathsf{g})$.
5. Publiez votre clé publique $\mathsf{pk} = (\mathsf{p}, \mathsf{g}, \mathsf{y})$.
   (Donnez la à votre voisin.)

*une liste des 10^8 nombres premiers est disponible sur : http ://www.bigprimes.net/archive/prime

anca.nitulescu@ens.fr

Chiffrement

Exercice 3 Récupérez la clef publique de votre voisin, puis choisissez un mot (5-10 lettres) à lui transmettre.

1. Codez le mot sous forme d'une séquence de nombre à l'aide de la table ASCII

2. Expliquez grâce à quelle propriété du chiffrement El Gamal on peut chiffrer lettre par lettre (on n'a pas besoin de découper le message en blocs de grande taille comme dans le cas de RSA).

3. Chiffrez avec la clé publique du destinataire :
   Pour chaque code ASCII, noté M :
   (a) Choisissez un aléa r.
   (b) Un nombre M est chiffré en une paire (C, D) par la formule :

$$(\mathsf{C}, \mathsf{D}) = (\mathsf{g}^{\mathsf{r}}, \mathsf{y}^{\mathsf{r}}\mathsf{M}) \ (\mathsf{mod}\ \mathsf{p})$$

   Exemple : Pour la lettre A avec l'aléa r :

$$(\mathsf{C}_{\mathsf{A}}, \mathsf{D}_{\mathsf{A}}) = (\mathsf{g}^{\mathsf{r}}, \mathsf{y}^{\mathsf{r}} \cdot 65) \ (\mathsf{mod}\ \mathsf{p})$$

   (c) Ecrivez le message chiffré et transmettez le à votre voisin.

Code dec.	Code bin.	Signif.
32	00100000	ESPACE
65	01000001	A
66	01000010	B
67	01000011	C
68	01000100	D
69	01000101	E
70	01000110	F
71	01000111	G
72	01001000	H
73	01001001	I
74	01001010	J
75	01001011	K
76	01001100	L
77	01001101	M
78	01001110	N
79	01001111	O
80	01010000	P
81	01010001	Q
82	01010010	R
83	01010011	S
84	01010100	T
85	01010101	U
86	01010110	V
87	01010111	W
88	01011000	X
89	01011001	Y
90	01011010	Z

*Vous utiliserez un calculateur à entier long, par exemple celui sur :
http ://www.jpvweb.com/cgi-bin/calculextcgi.py

Déchiffrement

Le destinataire d'un message chiffré (votre voisin) et vous même, vous déchiffrerez le message reçu en utilisant votre clé secrète x :

1. Calculez pour chacun des paires (C, D) : $\mathsf{M} = \mathsf{D} \cdot \mathsf{C}^{-\mathsf{x}} \ (\mathsf{mod}\ \mathsf{p})$.
2. Décodez la séquence obtenue en convertissant en caractères d'après la table ASCII.

• Attaques

RSA avec deux facteurs trop proche

Exercice 4 Supposons que l'entier n soit le produit de deux nombres premiers p et q proches (on peut toujours supposer que $\mathsf{p} > \mathsf{q}$).
On pose $\mathsf{t} = \frac{\mathsf{p}+\mathsf{q}}{2}$ et $\mathsf{s} = \frac{\mathsf{p}-\mathsf{q}}{2}$. Montrez que :

1. L'entier s est petit.
2. $\mathsf{n} = \mathsf{t}^2 - \mathsf{s}^2$.
3. t est légérement supérieur à la racine carrée de n.
4. On peut utiliser ces informations pour factoriser n.
5. Appliquez cet algorithme pour factoriser 899, 110417, puis 364957402.
6. Trouvez la clé secrète d correspondante à $\mathsf{pk} = (RSA, \mathsf{n} = 51983, \mathsf{e} = 17)$.

Algorithme de Fermat

(a) $\mathsf{t} \leftarrow \lceil \sqrt{\mathsf{n}} \rceil$
(b) $\mathsf{z} = 2$
(c) Tant que z n'est pas un carré :

i. $\mathsf{t} \leftarrow \mathsf{t} + 1$
ii. $\mathsf{z} \leftarrow \mathsf{t}^2 - \mathsf{n}$

(d) Retourner $\mathsf{p} = \mathsf{t} + \sqrt{\mathsf{z}}$.

RSA avec $\varphi(\mathsf{n})$ connu

Exercice 5 Bob utilise le protocole RSA et publie sa clé publique $\mathsf{n} = 187$ et $\mathsf{e} = 3$.
1. Encodez le message $\mathsf{m} = 15$ avec la clé publique de Bob.
2. En utilisant le fait que $\varphi(\mathsf{n}) = 160$, retrouvez la factorisation de n.
3. Retrouvez la clé privée d de Bob.

Cryptanalyse de RSA et factorisation

Exercice 6 Montrez que la connaissance d'un couple (e, d) aide à factoriser complétement le modulo n :

1. Un tel couple (e, d) fournit une racine carrée modulaire de 1 :
   (a) Montrez que $\mathsf{ed} - 1$ est pair.
   (b) Montrez que pour tout m : $\mathsf{m}^{\mathsf{ed}-1} = 1 \pmod{\mathsf{n}}$.
   (c) Conclure que $\mathsf{m}^{(\mathsf{ed}-1)/2}$ est une racine carrée de 1 $(\mathsf{mod}\ \mathsf{n})$.
2. Montrez que une racine carrée de 1 non triviale donne la factorisation de n en regardant l'équation $\mathsf{x}^2 - 1 = 0 \pmod{\mathsf{n}}$.
3. Appliquez le raisonement antérieur pour factoriser $\mathsf{n} = 2773$ dans le cas du protocol RSA à clé publique $(\mathsf{e}, \mathsf{n}) = (17, 2773)$ et clé privé $\mathsf{d} = 157$.

RSA avec modulo comun

Exercice 7 Bob et Charles utilisent le même modulo n pour leur clés RSA, car ils n'ont pas d'exigence de confidentialité l'un vis-à-vis de l'autre.

Bob et Charles ont pour clé publique RSA respectivement $(\mathsf{n}, \mathsf{e}_1)$ et $(\mathsf{n}, \mathsf{e}_2)$ avec e_1 et e_2 premiers entre eux. Alice envoie le meme message m aux deux. Alors, m sera crypté par les clés publiques RSA de Bob et Charles en c_1 et c_2. Expliquer comment Eve, qui intercepte les deux messages cryptés et qui connait les clés publiques de Bob et Charles, peut retrouver le message clair m.