Protocoles de cryptographie

TRc8 — R&T2A — TD N°2

Exercice 1 : *Algorithme RSA*

Le premier algorithme de chiffrement asymétrique et de signature proposé, l'algorithme `RSA`, a été publié en 1978 par Rivest, Shamir et Adleman. Sa sécurité repose sur la difficulté de *factoriser* des grands nombres. Le problème s'énonce ainsi :

Etant donné un entier n, produit de deux nombres premiers p et q, un entier y et un entier e premier avec $(p-1)(q-1)$,
trouver x, tel que $y = \equiv x^e \pmod{n}$

Ce problème st réputé difficile lorsque la *factorisation* de n est inconnue mais devient facile si p et q sont connus car la connaissance de ces deux nombres permet de déterminer l'entier d tel que :

$$ed \equiv 1\,(mod(p-1)(q-1))$$

On définit alors une fonction de `chiffrement` $x \mapsto x^e \bmod n$ et une fonction de `déchiffrement` $x \mapsto x^d \bmod n$ ainsi que la `clef publique` (e,n) et la `clef privée` (d,n).

L'algorithme `RSA` peut être utilisé pour assurer aussi bien la *confidentialité* des messages que leur *authentification*.

- CONFIDENTIALITÉ : la clef publique *chiffre* le message et la clef privée le *déchiffre*.
- AUTHENTIFICATION : la clef privée chiffre le message (on dit qu'elle le *signe*) alors que la clef publique déchiffre le message (on dit qu'elle *vérifie* la signature).

1. Quelle est la relation fondamentale entre la clef publique et la clef privée ?
2. En exploitant cette relation, montrer que la fonction de chiffrement proosée et bien l'inverse de la fonction de déchiffrement.
3. À partir de l'énoné du texte, détailler la procédure à suivre pour générer un couple (clef publique,clef privée).
4. Supposons qu'Alice et Bob veulent communiquer en utilisant RSA. Comment doivent-ils s'y prendre ?
5. Chiffrer le message 21 avec la clef publique (103,143). Le calcul peut être facilement fait à la main en remarquant que $21^4 \equiv 1 \pmod{143}$.
6. Déchiffrer le message obtenu avec la clef privée (7,143). Retrouve-t-on le message clair ?

Exercice 2 : *Signature et cryptage*

Soit un schéma d'authentification fondé sur une clef secrète fonctionnant comme suit. A et B sont seuls à connaître une clef qui paramètre une fonction C extrêmement difficile à inverser. Lorsque A veut s'assurer qu'il parle bien à B il lui lance un défi en tirant une chaîne aléatoire (nonce) R_A et demande à B de lui calculer $C(R_A)$. B fait de même pour s'assurer aussi qu'il parle bien à A. La Figure 2 décrit le protocole et une tentative de le simplifier.

1. Donnez un scénario avec le protocole de droite où une troisième personne arrive à se faire passer pour A auprès de B.

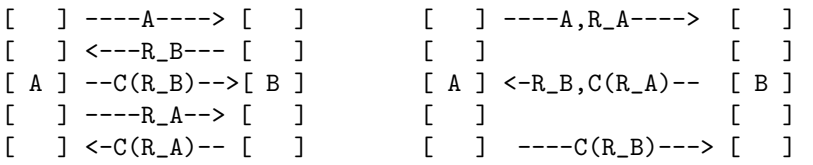

Fig 2 : à gauche le schéma d'authentification fondé sur une clef secrète, à droite une variante simplifiée (seul l'ordre des messages est changé, réduisant ainsi le nombre d'aller-retour).

Exercice 3 : *Authentification fondé sur une tièrce partie*

Considérant un protocole d'authentification utilisant un centre de distribution de clefs (KDC). Dans ce schéma très simple, chaque utilisateur partage avec le KDC une et une seule clef. L'authentification et l'échange de clef de session entre deux utilisateurs se déroulent via le KDC.

Par exemple, Si A veut communiquer avec B, il crée une clef de session K_{AB} et indique au KDC qu'il veut parler avec B en lui envoyant $\{A\}$ et $\{B, K_{AB}\}_{K_A}$, où K_A est la clef partagée entre A et le KDC. Le KDC déchiffre alors ce message et en construit un nouveau destiné à B contenant l'identité de A et la clef de session entre A et B ; ce message est chiffré avec la clef commune à B et au KDC (K_B) : $\{A, K_{AB}\}_{K_B}$. Maintenant, A peut envoyer un message à B chiffré avec K_{AB}.

Pour les questions 1 et 2, on ne tiendra pas compte d'attaques par rejeu d'un message.

1. Est-ce qu'un pirate peut se faire passer pour A auprès du KDC ? Expliquer et justifier votre réponse.
2. Est-ce que B est-il certain que le message provient bien du KDC ? Expliquer et justifier votre réponse.
3. À Quelle attaque ce protocole ne résiste-t-il pas ? Expliquer et justifier votre réponse.

   N.B : Imaginer qu'un pirate I ait effectué un travail pour A. Après avoir échangé une clef de session via le KCD, A envoie un message à son banquier B pour lui demander de verser la rétribution sur le compte de I. Que faire à la place de I pour augmenter ses gains ?
4. Comment améliorer le protocole sans augmenter le nombre d'échanges pour déjouer ce type d'attaque ?

Exercice 4 : *man-in-the-middle attack*

Considérant un protocole décrit par les règles d'échange de messages ci-dessous :

$$A \rightarrow B : \{A, N_a\}_{pub(B)}$$
$$B \rightarrow A : \{Na, N_b\}_{pub(A)}$$
$$A \rightarrow B : \{Nb\}_{pub(B)}$$

À la première étape du protocole, Alice envoie son nom A et un nombre engendré aléatoirement N_a, aussi appelé nonce. Ce message est chiffré avec la clef publique de B (notée $pub(B)$), donc seul l'agent Bob connaît la clef privée correspondant à la clef $pub(B)$. Bob reçoit le message $\{A, Na\}_{pub(B)}$ envoyé par Alice. Comme il a la clef privée lui permettant découvrir le message, il comprend qu'Alice veut lui parler et renvoie le nonce d'Alice ainsi qu'un autre nonce N_b qu'il vient d'engendrer, le tout chiffré avec la clef publique $pub(A)$ d'Alice (seconde étape). Alice reçoit le message $\{Na, Nb\}_{pub(A)}$ et reconnaît son nonce N_a. Elle en déduit que Bob lui a répondu et elle lui renvoie son nonce N_b chiffré avec sa clef publique pour lui signifier qu'elle connaît maintenant le message N_b (troisième étape). Lorsque Bob reçoit ce message, les deux agents pensent qu'ils sont seuls à connaître le nonce N_b et que celui-ci permet de les authentifier : lorsqu'Alice reçoit un message contenant N_b, elle en déduit qu'il vient de Bob et inversement.

1. Donnez un scénario d'attaque de type "man-in-the-middle" pour ce protocole.

Exercice 5 : *Authentification fondé sur une tièrce partie*

Considérant un protocole d'authentification utilisant un centre de distribution de clefs (KDC). Dans ce schéma très simple, chaque utilisateur partage avec le KDC une et une seule clef. L'authentification et l'échange de clef de session entre deux utilisateurs se déroulent via le KDC.

Par exemple, Si A veut communiquer avec B, il crée une clef de session K_{AB} et indique au KDC qu'il veut parler avec B en lui envoyant $\{A\}$ et $\{B, K_{AB}\}_{K_A}$, où K_A est la clef partagée entre A et le KDC. Le KDC déchiffre alors ce message et en construit un nouveau destiné à B contenant l'identité de A et la clef de session entre A et B ; ce message est chiffré avec la clef commune à B et au KDC (K_B) : $\{A, K_{AB}\}_{K_B}$. Maintenant, A peut envoyer un message à B chiffré avec K_{AB}.

1. Est-ce qu'un pirate peut se faire passer pour A auprès du KDC ? Expliquer et justifier votre réponse.

   Non, un pirate ne sera pas en mesure de se faire passer pour A auprès du KDC car il ne connait pas la clef secrète entre A et le KDC. Il ne pourra donc pas forger l'information signée $\{B, K_{AB}\}_{K_A}$ nécessaire dans le premier échange.

2. Est-ce que B est-il certain que le message provient bien du KDC ? Expliquer et justifier votre réponse.

   Comme tout client du KDC, B partage une clef secrète avec le KDC, notée K_B, que seules ces deux entités connaissent. Seul le KDC est donc en mesure de créer le message chiffré $\{A, K_{AB}\}_{K_B}$ reçu par B : le fait que le message déchiffré soit valide prouve qu'il a bien été émis par le KDC.

3. À Quelle attaque ce protocole ne résiste-t-il pas ? Expliquer et justifier votre réponse.

   Aucune mesure n'a été prise afin d'éviter une attaque par rejeu d'un message. En considérant l'exemple fourni, si l'attaquant I peut obtenir une copie de l'ordre de virement, il peut le renvoyer à volonté à B afin d'augmenter son profit.

   N.B : Imaginer qu'un pirate I ait effectué un travail pour A. Après avoir échangé une clef de session via le KCD, A envoie un message à son banquier B pour lui demander de verser la rétribution sur le compte de I. Que faire à la place de I pour augmenter ses gains ?

4. Comment améliorer le protocole sans augmenter le nombre d'échanges pour déjouer ce type d'attaque ?

   Plusieurs techniques peuvent être envisagées afin d'éviter une attaque par rejeu. On peut ajouter aux messages des numéros de séquence : un message, provenant d'un client A, reçu avec un numéro de séquence inférieur ou égal au dernier message reçu de A est jeté car il s'agit soit d'un rejeu, soit message dont le temps de transmission a été anormalement long.