Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms - By David Chaum

Présenté par Aurélien Monnet-Paquet

www.inria.fr

19 Mai 2016

Problème ?

- Comment garder confidentiel qui parle avec qui et quand ?

Problème ?

- Comment garder confidentiel qui parle avec qui et quand ?
- Cryptographie à clé publique

Notation

- K : Clé publique
- Inv(K) : Clé privée
- X : Message en clair

Notation

- K : Clé publique
- Inv(K) : Clé privée
- X : Message en clair
- $Inv(K)(K(X)) = K(Inv(K)(X)) = X$

Notation

- K : Clé publique
- Inv(K) : Clé privée
- X : Message en clair
- $Inv(K)(K(X)) = K(Inv(K)(X)) = X$
- R : Une chaîne de bits aléatoire

Notation

- K : Clé publique
- Inv(K) : Clé privée
- X : Message en clair
- $Inv(K)(K(X)) = K(Inv(K)(X)) = X$
- R : Une chaîne de bits aléatoire
- Le chiffrement du message par la clé publique :

$$K(R, X)$$

Hypothèses

Hypothèse 1

Personne ne peut déterminer quoi que ce soit sur les correspondances entre un ensemble d'éléments chiffrés et l'ensemble des éléments non chiffrés, ou créer des contrefaçons sans la chaîne aléatoire appropriée ou la clé privée.

Hypothèse 2

Alice souhaite envoyer un message à Bob :

- Alice chiffre le message M avec la clé publique (Ka) de Bob
- Alice ajoute l'adresse (A) de Bob au résultat
- Alice chiffre le tout avec la clé publique (K1) du premier serveur de mix

Alice souhaite envoyer un message à Bob :

- Alice chiffre le message M avec la clé publique (Ka) de Bob
- Alice ajoute l'adresse (A) de Bob au résultat
- Alice chiffre le tout avec la clé publique (K1) du premier serveur de mix

$$K1(R1, Ka(R0, M), A) \rightarrow Ka(R0, M), A.$$

Alice souhaite envoyer un message à Bob :

- Alice chiffre le message M avec la clé publique (Ka) de Bob
- Alice ajoute l'adresse (A) de Bob au résultat
- Alice chiffre le tout avec la clé publique (K1) du premier serveur de mix

$$K1(R1, Ka(R0, M), A) \rightarrow Ka(R0, M), A.$$

$$K1(R1, Ka(R0, M), A) \rightarrow Ka(R0, M), A.$$

- Le serveur de mix déchiffre ce qu'il reçoit avec sa clé privée
- Puis enleve la chaine R1 et delivre le reste

But d'un serveur de mix :

- Cacher les correspondances entre les éléments en entrée/sortie
- Cacher l'ordre d'arriver en fournissant des éléments de taille uniforme en sortie
- Traiter une et une seule fois un lot

Si R1 contient un horodatage, le serveur ne conserve pas de copie des lots

Signature

Cascade

Comment répondre en gardant l'adresse d'Alice anonyme ?

Former une adresse anonyme de retour :

$$K1(R1, Ax), Kx$$

- Ax est l'adresse réelle d'Alice

Comment répondre en gardant l'adresse d'Alice anonyme ?

Former une adresse anonyme de retour :

$$K1(R1, Ax), Kx$$

- Ax est l'adresse réelle d'Alice
- Kx est une clé publique choisie pour l'occasion

Comment répondre en gardant l'adresse d'Alice anonyme ?

Former une adresse anonyme de retour :

$$K1(R1, Ax), Kx$$

- Ax est l'adresse réelle d'Alice
- Kx est une clé publique choisie pour l'occasion
- R1 est une clé / chaîne aléatoire à des fins d'étanchéité

$$K1(R1, Ax), Kx(R0, M) \rightarrow Ax, R1(Kx(R0, M))$$

- $Kx(R0, M)$ est

$$K1(R1, Ax), Kx(R0, M) \rightarrow Ax, R1(Kx(R0, M))$$

- $Kx(R0, M)$ est
- $K1(R1, Ax)$ est le chiffrement de l'adresse d'Alice + la clé R1 avec l'adresse publique du premier serveur

En utilisant une cascade de serveurs

$$K1(R1, K2(R2, ..., A...)), Kx(R0, M)$$

- Avec A = $K < n-1 > (R < n-1 >, Kn(Rn, Ax))$

Alice peut recevoir un accusé de réception sur le message qu'elle envoie à Bob :

- L'adresse réelle d'Alice est étendu avec une autre adresse anonyme (pour Alice et Bob)
- Envoi de l'accusé une fois que le dernier serveur a envoyé le message
  - Adresse de livraison du message
  - Le message
  - Peut être signé par tous les serveurs intermédiaire

Définition

Un "pseudonyme" numérique est une clé publique utilisée pour vérifier les signatures effectuées par le titulaire anonyme de la clé privée correspondante.

Comment ?

Une autorité est chargé de tenir a jour une liste de pseudonymes

Chaque demande d'acceptation :

- Peut être soumis par le system de mail anonyme
- Doit contenir la clé publique et le pseudonyme souhaiter
- Peut être pour une liste particulière soumise a un vote
- Peut être accepter ou refuser par l'autorité

1

1