N’essaie pas de tricher !

protocoles de sécurité

Qu’est-ce qu’un protocole ?

Un protocole est un ensemble de règles que des programmes utilisent pour communiquer.

Les protocoles de sécurité

Souvent, pour illustrer un protocole de sécurité, on raconte une histoire, où tous les personnages jouent toujours le même rôle.

Alice,
Bob,
Carole,
Dave,

sont les principaux acteurs.

Ève enregistre tout.

Mallory est malicieuse

Trent est très écouté, c'est un tiers de confiance ou un garant.

Les protocoles de sécurité

Tout le monde se méfie de tout le monde.

Un protocole doit être robuste à toute attaque (sécurité).

Il est très difficile de prédire la robustesse d'un protocole. En général, son inventeur explique pourquoi il le croit robuste et le propose à la communauté des experts qui essaient de trouver des attaques. S'il résiste, il est considéré comme bon.

S'engager sur un nombre (I)

Première histoire

Alice qui est en $1^{\mathrm{ere}}\mathrm{S}_1$ connaît le sujet du devoir sur table de $1^{\mathrm{ere}}\mathrm{S}_2$ de demain. Elle veut prouver à Bob qu'elle le connaît vraiment, mais elle ne veut pas lui donner la réponse maintenant, mais seulement demain après-midi.

Bob est prêt à parier 100 F.

S’engager sur un nombre (II)

Deuxième histoire

Alice connaît l’action en bourse qui va monter le plus le mois prochain, elle veut montrer à Bob qu’elle le sait, mais elle ne veut pas que Bob puisse agir sur le cours.

S’engager sur un nombre (III)

Le scénario

Alice doit s’engager auprès de Bob sur un nombre.

Alice ne pourra plus changer ce nombre.

Bob ne peut pas découvrir la valeur de ce nombre sans l’accord d’Alice.

Alice et Bob communiquent par un réseau informatique.

Cryptographie

Pour crypter, on a besoin d'une clé, la clé de cryptage.

La fonction de cryptage est une fonction E_k.

Si on ne connaît pas la clé de décryptage, on ne peut pas calculer M, connaissant $E_k(M)$.

Crypter un nombre M, c'est fabriquer $E_k(M)$.

Un système de cryptographie est symétrique si la clé de décryptage est la même que la clé de décryptage.

Un bon système cryptographique doit résister le plus longtemps possible aux meilleures attaques, (plusieurs siècles ?).

Alice s'engage sur le nombre N

Un protocole à base de cryptographie

Avant (aujourd'hui),

- Bob fabrique un nombre au hasard p et l'envoie à Alice.
- Alice fabrique une clé de cryptage k au hasard.
- Alice calcule $e = E_k(p, N)$ et l'envoie à Bob.

Après, (demain, dans un mois, ...)

- Alice envoie la clé de cryptage k à Bob.
- Bob décrypte $E_k(p, N)$.

Alice s'engage sur le nombre N

Justification du protocole à base de cryptographie

Comme Bob fabrique le nombre p, Alice ne peut pas avoir préparé son coup et fabriqué des clés pour les différents N.

p est appelé un nonce et garantit la fraîcheur.

Fonctions à sens unique

Une fonction à sens unique $SensUnique$ est une fonction pour laquelle

- on peut calculer $y = SensUnique(x)$ quand on connaît x,
- mais pas pas x quand on connaît y.

Alice s'engage sur le nombre N

Un protocole à base de fonction à sens unique

Avant (aujourd'hui),

- Alice et Bob se mettent d'accord sur une fonction $SensUnique$.
- Alice crée deux nombres au hasard p et q,
- Alice calcule la valeur $e = SensUnique(p, q, N)$,
- Alice envoie le nombre e.

Après, (demain, dans un mois, ...)

- Alice envoie (q, N) à Bob,
- Bob vérifie que $e = SensUnique(p, q, N)$.

Alice s'engage sur le nombre N

Justification du protocole à base de fonction à sens unique

– Comme la fonction est à sens unique, Bob connaît e,

mais Bob ne connaît ni p, ni N.

– Alice fournit p comme garantie de fraîcheur.

– Alice doit garder un nombre q caché, car sinon Bob pourrait calculer

  – $e = SensUnique(p, 1)$,

  – $e = SensUnique(p, 2)$,

  – etc.

et trouver le N tel que $e = SensUnique(p, N)$.

Alice et Bob jouent à pile ou face

Protocole à base de fonction à sens unique

- Alice choisit un nombre x au hasard.
- Alice calcule $y = SensUnique(x)$.
- Alice envoie y à Bob.
- Bob doit deviner si x est pair ou impair.
- Si Bob a correctement deviné, le résultat final est pile, sinon c'est face.
- Alice annonce le résultat et envoie x à Bob.
- Bob vérifie que $y = SensUnique(x)$.

Clés publiques et clés privées

Dans un système de clés asymétriques, on peut distinguer :

- une clé publique :
  - tout le monde peut m'envoyer des messages cryptés que je serai le seul à décrypter.
- une clé privée :
  - je peux décrypter des messages que l'on m'envoie cryptés avec ma clé publique,
  - je peux crypter des messages avec ma clé privée que mes destinataires décrypteront avec ma clé publique (signature).

Ma clé publique sous pgp

```
Type Bits/KeyID     Date       User ID
pub   512/7AC3151D 1999/10/19 Pierre.Lescanne@ens-lyon.fr
```


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQBNAzgMissAAAECAKYtbXrv4PTA3V42wSe2zP3nJKirAHOrxwfXsZcVXTRXhpUk
E5TPnUK3zFiYw7xZdb5eho0H86/vTZ6bunrDFR0ABRG0G1BpZXJyZS5MZXNjYW5u
ZUBlbnMtbHlvbi5mcokAVQMFEDgMistNnpu6esMVHQEBc6EB/0NnFX+IO6HV9eR0
WjKYyztTs4mUax7k+nDhVdzXnplvQQRZZyJzrK5FurQUPeC+FL1QpsJPeUpSywN/
dsvyJ64=
=4p6G
-----END PGP PUBLIC KEY BLOCK-----
```

Quelques concepts fondamentaux

La sécurité sur le Web cherche à garantir les propriétés suivantes :

- confidentialité, y compris l'absence ce fuite d'information,
- intégrité,
- disponibilité.

et à mettre en œuvre deux fonctions :

- l'authentification,
- la non répudiation.

Ce qu'on a vu

- les protocoles
- la cryptographie et le cryptage,
- les clés : publiques, privées, symétriques,
- les fonctions a sens unique,
- les nonces, la fraîcheur.

Ce qu'il nous resterait à voir

- Les protocoles d'échanges de clés de session,
- les protocoles à information nulle,
- les algorithmes cryptographiques :
  - DES,
  - RSA,
  - courbes elliptiques.

Ce qu'il nous resterait à voir (suite)

- les méthodes de vérification de protocoles,
  - les preuves à la main dans des logiques de la croyance,
  - les énumérations de modèles,
  - la démonstration automatique ou assistée de théorèmes.
- Les critères communs de certification de systèmes informatiques de sécurité,
- etc.