LE CHIFFREMENT HYBRIDE :

1. Le chiffrement hybride :

Le chiffrement hybride consiste à associer deux types de chiffrement : un chiffrement symétrique (type AES) et un chiffrement asymétrique (type RSA). Rappelons la nature de ces deux types de chiffrement ;

- **Le chiffrement symétrique** : Une seule et même clé sert à chiffrer et à déchiffrer les données (exemple : AES). Ce mode de chiffrement est très rapide et efficace pour chiffrer de grandes quantités de données, mais pose un problème de distribution sécurisée de la clé.

- **Le chiffrement asymétrique** : Il utilise une paire de clés, une publique pour chiffrer et une privée pour déchiffrer (exemple : RSA). Il résout le problème de distribution des clés, mais il est beaucoup plus lent, surtout pour chiffrer des volumes importants de données.

Le chiffrement RSA a été abordé dans la fiche n° 7 d'initiation à la cryptographie et le chiffrement AES dans l'une des fiches sur la cryptographie moderne.

2. Principe de fonctionnement du chiffrement hybride

Le chiffrement hybride combine ces deux méthodes pour tirer parti de leurs forces tout en minimisant leurs inconvénients. Le principe général de fonctionnement est le suivant :

- **Génération d'une clé de session symétrique** :

Le chiffreur génère une clé symétrique temporaire (appelée **clé de session**), souvent à l'aide d'un algorithme.

- **Chiffrement des données avec la clé symétrique** :

La clé de session est utilisée pour chiffrer les données du message clair avec un algorithme de chiffrement symétrique rapide et efficace.

- **Chiffrement de la clé de session avec un algorithme asymétrique** :

La clé symétrique est ensuite chiffrée à l'aide d'un algorithme asymétrique (comme RSA) et de la clé publique du destinataire. Cette étape garantit que seule la personne possédant la clé privée correspondante peut déchiffrer la clé symétrique.

- **Transmission** :

Les données chiffrées du message et la clé de session chiffrée sont envoyées au destinataire.

- **Déchiffrement** :

Le destinataire déchiffre d'abord la clé symétrique avec sa clé privée RSA.

Il utilise ensuite cette clé symétrique pour déchiffrer le message.

3. Illustration pratique du chiffrement hybride avec Alice et Bob :

- Bob veut adresser un message à Alice

- Alice dispose d'une clé pour le chiffrement en RSA. Elle a donc diffusé publiquement N et son exposant public e. Bien entendu, elle garde toujours secret son exposant privé d.

Opérations à effectuer par Bob :

- Créer le message en clair.

- Créer une clé symétrique, appelée « clé de session ». Cette clé est généralement plus courte que le message clair.

- Chiffrer le message clair avec cette clé de session, par exemple avec un chiffrement AES.

- Chiffrer ensuite la clé de session par un chiffrement RSA avec la clé publique d'Alice.

- Adresser à Alice en un seul fichier le message chiffré avec la clé de session et la clé de session chiffrée en RSA avec la clé publique.

Opérations à effectuer par Alice :

Lorsqu'elle reçoit ce fichier, Alice déchiffre la clé de session grâce à sa clé privée d, puis déchiffre le message original avec la clé de session.

4. Les avantages du chiffrement hybride

- **Efficacité :** L'algorithme symétrique est utilisé pour chiffrer les données volumineuses de manière rapide, tandis que l'algorithme asymétrique est utilisé uniquement pour protéger la clé de session, ce qui minimise l'impact de sa lenteur.

- **Sécurité de la clé :** L'utilisation d'un chiffrement asymétrique garantit que la clé symétrique ne peut être déchiffrée que par le destinataire prévu, ce qui résout le problème de distribution de clé dans le chiffrement symétrique.

- **Confidentialité :** Même si quelqu'un intercepte les données, il ne peut pas les déchiffrer sans la clé de session, qui elle-même est protégée par le chiffrement asymétrique

5. Les limites de ce type chiffrement

Bien que très efficace, le chiffrement hybride n'est pas exempt d’incertitudes :

Gestion des clés : Si une clé privée est compromise, toutes les sessions passées et futures pourraient être déchiffrées.

Attaques : Les attaques sur les algorithmes RSA ou d'autres algorithmes asymétriques peuvent compromettre la sécurité globale du chiffrement hybride. Cependant, en utilisant des tailles de clés suffisamment grandes et des protocoles de chiffrement modernes (comme les courbes elliptiques), ces attaques sont atténuées.

Un chiffre hybride actuel utilise le plus souvent un algorithme symétrique de type AES avec une clé de session de 128 symboles binaires (bits) qui permet de chiffrer de longs messages de manière sûre, associé à un RSA qui utilise des clés de 1024 à 2048 bits.

6. Les applications courantes du chiffrement hybride

Le chiffrement hybride est la méthode de base dans de nombreuses applications de sécurité, telles que :

- **SSL/TLS** : Utilisé pour sécuriser les connexions Internet (par exemple, HTTPS).
- **PGP (Pretty Good Privacy)** : Utilisé pour le chiffrement des e-mails.

*****

***

*