REPUBLIQUE DU SENEGAL

Un Peuple-Un But-Une Foi

****

Ministère de l'Enseignement Supérieur de la Recherche et de l'innovation

****

DIRECTION DE L'ENSEIGNEMENT SUPERIEUR PRIVE

UNIPRO

FORMATION EN ALTERNANCE

Adresse: Mermoz Comico 2 / **Tel**: 33 825 23 78 / **Site**: www.uniprosenegal.com

EXPOSÉ

Option : Génie Informatique

THEME

CRYPTOGRAPHIE ASYMÉTRIQUE

Présentés par :

Rémy Mendy
Fatoumata Diarrayi Diallo
Mamadou Lamine Diallo
Mouhamed
Mamadou Maouloudou Diallo

Professeur :

M. GUEYE

Année Académique 2020-2021

UNIPRO
FORMATION EN ALTERNANCE

PLAN

- INTRODUCTION
- HISTORIQUE
- PRINCIPE DE FONCTIONNEMENT
- DÉFINITION
- AVANTAGE ET INCONVÉNIENT
- MISE EN PLACE D'UNE CLÉ DE CHIFFREMENT RSA AVEC OPENSSL
- CONCLUSION

INTRODUCTION

La cryptographie, ou **cryptologie**, est la pratique et l'étude de techniques de communication sécurisée en présence de tiers appelés adversaires. Plus généralement, la cryptographie consiste à construire et à analyser des protocoles qui empêchent des tiers ou le public de lire des messages privés; Divers aspects de la sécurité de l'information tels que la confidentialité des données, l'intégrité des données, l'authentification et la non-répudiation sont au cœur de la cryptographie moderne.

Parmi ces techniques nous avons la cryptographie symétrique et asymétrique qui est l'objet de notre étude.

La cryptographie asymétrique ou à clé publique est un domaine de la **cryptographie** où il existe une distinction entre des données *publiques* et *privées*, en opposition à la **cryptographie symétrique** où la fonctionnalité est atteinte par la possession d'une donnée secrète commune entre les différents participants.

La cryptographie asymétrique peut être illustrée avec l'exemple du *chiffrement à clef publique et privée*, qui est une technique de **chiffrement**, c'est-à-dire que le but est de garantir la confidentialité d'une donnée. Le terme asymétrique s'applique dans le fait qu'il y a deux **clefs de chiffrement** (que l'utilisateur qui souhaite recevoir des messages fabrique lui-même), telles que si l'utilisateur utilise une première clef dans un **algorithme** dit « de chiffrement », la donnée devient inintelligible à tous ceux qui ne possèdent pas la deuxième clef, qui peut retrouver le message initial lorsque cette deuxième clef est donnée en entrée d'un algorithme dit « de déchiffrement ».

Par convention, on appelle la clef de déchiffrement la clef privée et la clef de chiffrement la clef publique.

INTRODUCTION

La clef qui est choisie privée n'est jamais transmise à personne alors que la clef qui est choisie publique est transmissible sans restrictions.

Ce système permet deux choses majeures :

1.chiffrer le message à envoyer : l'expéditeur utilise la clef publique du destinataire pour chiffrer son message. Le destinataire utilise sa clef privée pour déchiffrer le message de l'expéditeur, garantissant la confidentialité du contenu ;

2.s'assurer de l'authenticité de l'expéditeur : L'expéditeur utilise sa clef privée pour chiffrer un message que le destinataire peut déchiffrer avec la clef publique de l'expéditeur ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message.

HISTORIQUE

Le concept de cryptographie à clef publique — autre nom de la cryptographie asymétrique — est généralement attribué à Whitfield Diffie et à Martin Hellman qui l'ont présenté au public à la National Computer Conference en 1976, puis publié quelques mois plus tard dans New Directions in Cryptography. Le concept aurait cependant été découvert indépendamment par d'autres chercheurs à la même époque. Ralph Merkle aurait fait la même découverte à la même époque, même si ses articles ne furent publiés qu'en 1978.

PRINCIPE DE FONCTIONNEMENT

La **cryptographie asymétrique**, ou *cryptographie à clef publique* est fondée sur l'existence des **fonctions à sens unique** et à **brèche secrète**.

Les fonctions à sens unique sont des fonctions mathématiques telles qu'une fois appliquées à un message, il est extrêmement difficile de retrouver le message original.

L'existence d'une brèche secrète permet cependant à la personne qui a conçu la fonction à sens unique de décoder facilement le message grâce à un élément d'information qu'elle possède, appelé clef privée.

PRINCIPE DE FONCTIONNEMENT

Supposons que Ndiaye souhaite recevoir un message secret de Traoré sur un canal susceptible d'être écouté par un attaquant passif Diallo :

Ndiaye transmet à Traoré une fonction à sens unique pour laquelle elle seule connait la brèche secrète ;

Traoré utilise la fonction transmise par Ndiaye pour chiffrer son message secret ;

Ndiaye réceptionne le message chiffré puis le décode grâce à la brèche secrète ;

Si Diallo réceptionne également le message alors qu'il circule sur le canal public, elle ne peut le décoder, même si elle a également intercepté l'envoi de la fonction à sens unique, car elle n'a pas connaissance de la brèche secrète.

PRINCIPE DE FONCTIONNEMENT

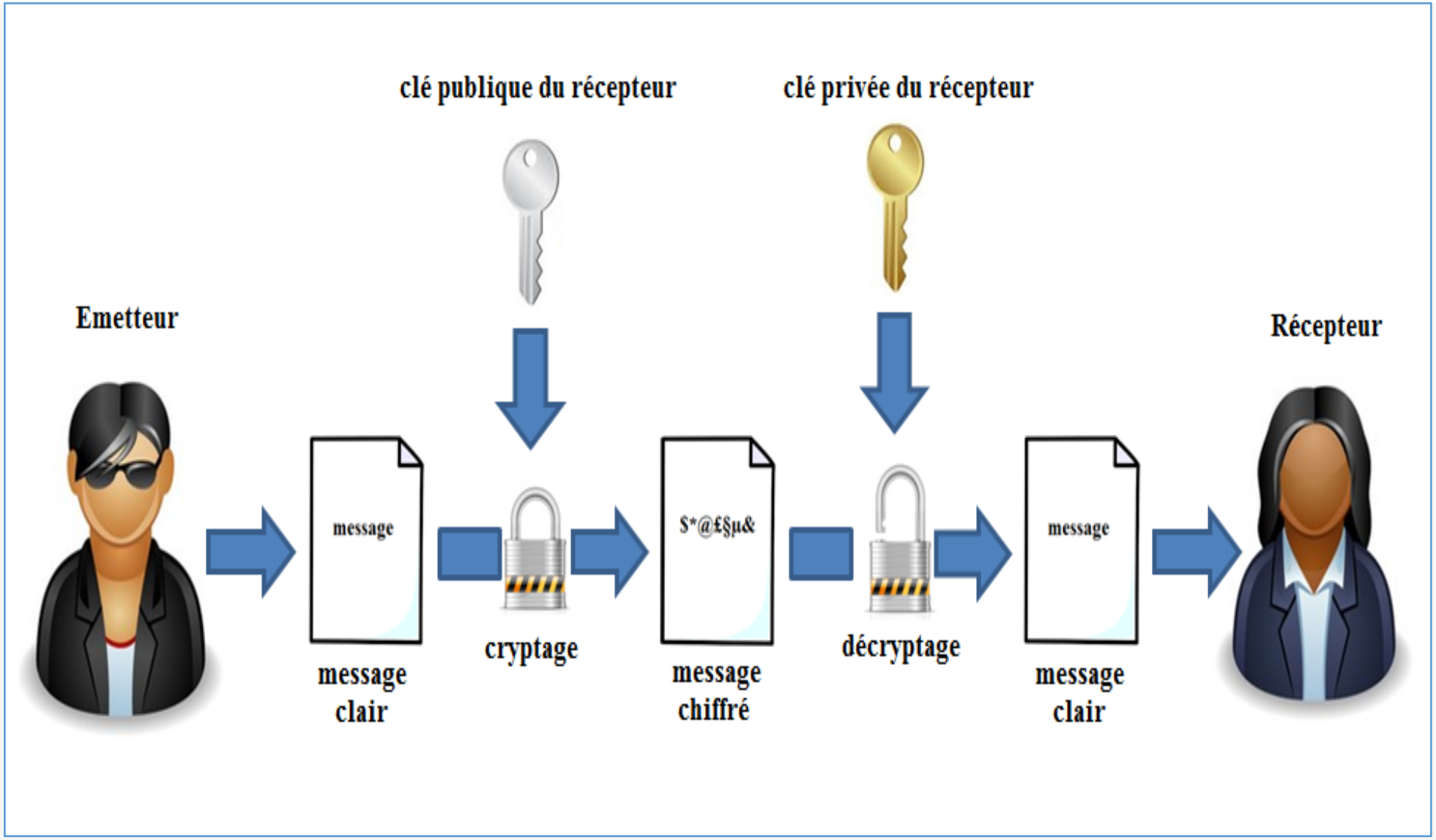
La terminologie classiquement retenue est :

pour la fonction à sens unique : « clef publique » ;

pour la brèche secrète : « clef privée ».

En pratique, sont utilisées des fonctions de chiffrement classiques, les termes « clef publique » et « clef privée » correspondant alors à des paramètres employés pour ces fonctions.

PRINCIPE DE FONCTIONNEMENT



DÉFINITION :

La cryptographie asymétrique (Public-key cryptography) est un technique utilisée pour protéger des fichiers, des registres et des disques entiers contre les accès non autorisés ainsi que pour échanger des messages secrets. Pour cela, on utilise des clés (key), pour le chiffrement et le déchiffrement des données.

AVANTAGE ET INCONVENIENT :

Les algorithmes de cryptographie asymétriques sont plus complexes que les algorithmes de cryptographie symétriques, ils sont donc plus lents et nécessitent plus de puissance de traitement. Cependant, ils sont aussi beaucoup plus sûrs. La clé publique peut être distribuée à toute personne susceptible d'être intéressée par le cryptage d'un message, mais la clé privée n'est jamais divulguée, ce qui ne la rend pas vulnérable aux pirates informatiques. Les données ne peuvent être cryptées qu'avec la clé publique et décryptées avec la clé privée, ce qui signifie qu'une fois le cryptage effectué, aucun expéditeur ne peut les décrypter sans clé privée.

MISE EN PLACE UNE CLE RSA AVEC OPENSSH :

Descriptions Openssh

OpenSSH est une version libre de la famille d'outils du protocole Secure Shell (SSH) pour le contrôle à distance ou le transfert des fichiers entre les ordinateurs. Les outils traditionnels utilisés pour accomplir ces fonctions tels que telnet ou rcp ne sont pas sécurisés et transmettent le mot de passe utilisateur en clair lors de leurs utilisations. OpenSSH fournit un démon de serveur et des outils pour les clients afin de sécuriser le contrôle à distance et chiffré les opérations de transfert de fichiers.

CONCLUSION :

Différence entre cryptage symétrique et asymétrique:

Le cryptage symétrique est la méthode d'utilisation des mêmes clés cryptographiques pour les cryptages de texte en clair et le décryptage de texte crypté. ***Le cryptage asymétrique*** est la méthode d'utilisation d'une paire de clés: la clé publique, largement diffusée, et une clé privée, connue uniquement du propriétaire.

Comme une seule clé est utilisée dans les deux opérations, le chiffrement symétrique est simple. Cependant, le cryptage asymétrique est plus complexe car il utilise des clés distinctes pour les deux opérations.

Le cryptage asymétrique est plus lent que le cryptage symétrique, qui a une vitesse d'exécution plus rapide.

RC4, AES, DES et 3DES sont des algorithmes courants de chiffrement symétrique. **Diffie-Hellman et l'algorithme RSA** sont des algorithmes de chiffrement asymétriques courants.

CONCLUSION :

En conclusion le cryptage symétrique et asymétrique sont deux techniques utilisées dans le cryptage et le décryptage. La différence entre le cryptage symétrique et asymétrique réside dans le fait que le cryptage symétrique utilise la même clé pour le cryptage et le décryptage, tandis que le cryptage asymétrique utilise deux clés différentes pour le cryptage et le décryptage.

UNIPRO

FORMATION EN ALTERNANCE

MERCI POUR VOTRE ATTENTION

https://www.formation-unipro.com