TD 5: Gestion de clés et protocoles

1 Les protocoles de Diffie Hellman

1. Rappelez à quoi sert le protocole de Diffie-Hellman et dites pourquoi il est utilisé.
`OpenSSL` implémente 3 versions du protocole de Diffie-Hellman:

- **Anonymous Diffie-Hellman** uses Diffie-Hellman, but without authentication and the keys used in the exchange are not authenticated.
- **Fixed Diffie-Hellman** embeds the server's public parameter in the certificate, and the CA then signs the certificate. That is, the certificate contains the Diffie-Hellman public-key parameters, and those parameters never change.
- **Ephemeral Diffie-Hellman** uses temporary, public keys. Each run of the protocol uses a different public key. The authenticity of the server's temporary key can be verified by checking the signature on the key. Because the public keys are temporary, a compromise of the server's long term signing key does not jeopardize the privacy of past sessions.

2. Dites sur quelle(s) versions une attaque de l'homme du milieu peut-elle réussir et décrivez son fonctionnement en détail.

2 Version de Needham-Schroeder publique

Dans la version 4 de Kerberos présentée en cours, le protocole utilisé est celui de Needham-Schroeder. Pour l'authentification, celui-ci utilise un système de chiffrement à clé secrète. On rappelle ci-dessous son fonctionnement : Charles (le client C) souhaite communiquer secrètement avec Serge (le serveur S) en se faisant délivrer un certificat par Théo (le tiers de confiance T)

a). Charles s'adresse à Théo en clair en lui envoyant C, S

b). Théo envoie à Charles, en chiffrant avec la clé de C

- S, une clé de session K
- un certificat chiffré avec la clé de Serge contenant C et la clé K

c). Charles transmet le certificat à Serge

(1) Montrez comment réaliser ce protocole simplifié en utilisant de la cryptographie à clé publique (chiffement et signature).

(2) Programmez le protocole à clé publique en utilisant la libraire `Cryptography` de `Python` [optionnel]

(3) Pourquoi ne peut-on pas se passer entièrement de chiffres à clé secrète?

(4) Discutez de la sûreté de votre protocole, notamment pour des attaques comme celle de «l'homme du milieu» et du rejeu.

3 Protocole LD

On s'intéresse au protocole de la Figure 1; p est un nombre premier et α un générateur de $\mathbb{Z}_p^\star$:

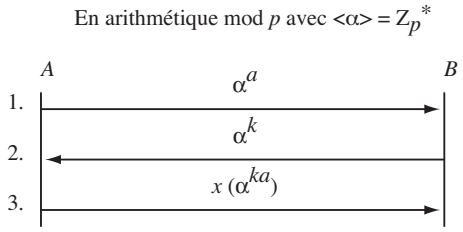

Figure 1: Protocole LD

(1) Montrez comment B retrouve la valeur x après l'étape 3 en justifiant brièvement votre réponse.

(2) En justifiant votre réponse, dites à quoi peut servir ce protocole.

(3) Grâce à une attaque passive, vous avez obtenu les valeurs suivantes: 90 pour la première communication, 81 pour la seconde et 89 pour la troisième. Appliquez l'algorithme de Shanks pour trouver le logarithme discret de $y = 90$ en base 3 dans $\mathbb{Z}_{101}^\star$. On rappelle que l'inverse multiplicatif de 3 dans $\mathbb{Z}_{101}^\star$ est 34 et on s'aidera du tableau des petits pas et grands pas suivant:

i	0	1	2	3	4	5	6	7	8	9	10
α^i	1	3	9	27	81	41	22	66	97	89	
$y(\alpha^{-10i})$	90	48	66	15	8	11	53	35	86	93	90

En expliquant votre calcul, donnez la valeur du logarithme discret de 90 en base 3 dans $\mathbb{Z}_{101}^\star$.

(4) Quelle est la valeur de $\alpha^{(ka)}$?

(5) Quelle était la valeur de x dans la troisième étape du protocole?

(6) Transformez ce protocole dans un groupe additif et décrivez comment vous en feriez l'attaque.