→ La qualité d'un cryptosystème s'évalue aujourd'hui sur le **compromis entre rapidité et sécurité**. Comment peut-on développer une application concrète du cryptosystème d'El Gamal et qu'en est-il de sa qualité ?

La cryptologie consiste en l'étude des techniques destinées à **protéger l'information contre une attaque malveillante**. Trois acteurs font partie d'un système cryptologique : l'**émetteur** et le **destinataire du message** mais il y a aussi l'**adversaire**, c'est-à-dire un attaquant voulant accéder aux données cryptées.

Un système cryptographique est un ensemble de **protocoles et d'algorithmes** qui permettent à l'émetteur et au destinataire **d'échanger des données de manière sûre**.

Parmi les services offerts par la cryptographie, nous retrouvons le **chiffrement** qui est l'utilisation traditionnelle de cette dernière ayant pour but **rendre un message secret**.

La sécurité de la cryptographie repose sur le **secret de la clé** permettant de **chiffrer et déchiffrer** le message. On distingue 2 types de clés : les **clés publiques** (auxquelles tout le monde a accès) et les **clés privées** (secrètes). Un des premiers problèmes de sécurité est de pouvoir **échanger la clé** entre l'émetteur et le destinataire **de manière confidentielle.**

Publié en 1976, le **protocole Diffie-Hellman** est la première **méthode d'échange de clés** utilisant **un système** de **clés publiques**. Il permet à un émetteur et un destinataire d'échanger une clé secrète commune par l'intermédiaire d'une clé publique. Sa mise en place a permis de simplifier la distribution des clés, notamment sur les réseaux ouverts comme Internet.

Le chiffrement d'El Gamal est un **protocole de cryptographie asymétrique** (c'est-à-dire qui utilise des clés publiques et privées). Il s'agit une **variante du protocole Diffie-Hellman** dans lequel l'émetteur et le récepteur s'échangent en plus d'une clé publique, un **message crypté**.

La **sécurité du système** de cryptage est basée sur le **calcul du logarithme discret** qui est un **problème mathématique réputé difficile**. Les seuls algorithmes connus permettant de résoudre ce problème sont **inapplicables en un temps raisonnable.** Cependant, plusieurs modèles d'attaques existent pour contourner cette difficulté, notamment en **exploitant la connaissance de messages clairs et cryptés**.

Enfin, dans le but de **garantir l'authenticité** des clés publiques utilisées ainsi que celle des messages, un **mécanisme de signature** peut être mis en place : les **clés sont ainsi assorties d'un certificat** permettant la **vérification de sa provenance**, notamment pour contrer une attaque classique dite de « l'homme du milieu ».