

---

# SÉCURITÉ DES SYSTÈMES DE CHIFFREMENTS À CLÉ PUBLIQUE BASÉS SUR LE PROBLÈME DU LOGARITHME DISCRET

*par*

Robert Rolland

---

**Résumé.** — Dans une première partie, nous faisons un tour d’horizon rapide de l’organisation ainsi que des principaux problèmes de la cryptographie. Dans la deuxième partie, nous étudions les problèmes liés au logarithme discret dans un groupe cyclique, en particulier les problèmes CDH et DDH. Enfin, dans la troisième partie, nous donnons les méthodes classiques utilisées dans le domaine de la sécurité prouvée, et ceci sur l’exemple du chiffrement à clé publique. Nous terminons par une suite d’exemples de systèmes de chiffrement à clé publique dont les sécurités croissantes reposent sur le problème DDH : chiffrement d’Elgamal, chiffrement construit à partir de ce dernier par la méthode de Fujisaki-Okamoto, chiffrement de Cramer-Shoup.

## Table des matières

<b>Partie I. Le cadre général</b> .....	2
1. Introduction, exemples.....	2
2. Quelques précisions et remarques.....	10
<b>Partie II. Les problèmes liés au logarithme discret</b>	12
3. Les problèmes DLP, CDH et DDH.....	12
4. Approfondissement du problème DDH.....	14

---

*Classification mathématique par sujets (2000).* — 94A60, 11T71.

*Mots clefs.* — cryptographie, logarithmes discrets, problème de Diffie-Hellman, sécurité prouvée, chiffrement à clé publique, chiffrement d’Elgamal, méthode de Fujisaki-Okamoto, chiffrement de Cramer-Shoup.

<b>Partie III. Sécurité de systèmes liés au problème du logarithme discret</b> .....	23
5. Sécurité au sens de Shannon.....	23
6. Généralités sur la sécurité des chiffrements à clé publique.....	24
7. Formalisation des notions de sécurité des cryptosystèmes à clé publique.....	30
8. Les exemples de chiffrement basés sur le logarithme discret.....	36
Références.....	40

## PARTIE I LE CADRE GÉNÉRAL

### 1. Introduction, exemples

Afin de bien situer le problème dans son contexte, nous allons tout d'abord faire un bref tour d'horizon de l'organisation de la cryptologie moderne. Evidemment ce tour d'horizon est loin d'être complet. Son intérêt est de présenter les divers niveaux auxquels se situent les éléments que nous développerons par la suite. Pour les questions générales de cryptographie on pourra se référer à [1].

**1.1. Les débuts de la cryptologie moderne.** — Au cours de la deuxième moitié du vingtième siècle, la cryptographie a quitté son statut essentiellement militaire. Les développements des divers moyens technologiques et le foisonnement des applications impliquant des échanges de données sécurisées en milieu ouvert ont largement étendu le champ des activités qui en relèvent. Si on veut se faire une idée assez nette de ce que pouvait être la cryptographie et les pratiques cryptographiques jusqu'à la fin de la deuxième guerre mondiale, on peut lire le texte d'Auguste Kerckhoffs : « La cryptographie militaire, Journal des Sciences militaires, vol. IX, pp. 5-38, Janvier 1883 et pp. 161-191, Février 1883 »