ALGORITHMIQUE DE LA CRYTPTOGRAPHIE À CLÉ PUBLIQUE

KARIM BELABAS

(1) Initiation au système Pari/GP. Représentation machine des corps finis, des courbes elliptiques.

(2) Ordres de complexité pratiques. Exemples : opérations en multiprécision, algorithme d'Euclide, exponentiation modulaire, opérations sur les matrices, complexité actuelle des tests de primalité, factorisation et logarithme discret.

(3) Primalité et factorisation.

Divisions successives, théorèmes de Fermat, et Euler-Fermat, nombres pseudo-premiers forts, test de Rabin-Miller, description détaillée de l'exponentiation modulaire, faux témoins.

Preuves de primalité : Pocklington-Lehmer. Exemple Mersenne et Fermat. Factorisation : méthode rho de Pollard, méthode $p-1$ (première et deuxième phase), utilisation du sous-groupe d'ordre $p+1$ du corps à p^2 éléments. Méthodes sous-exponentielles de factorisation : Dixon, crible quadratique.

(4) Courbes elliptiques (utilité pour la factorisation, la primalité, le logarithme discret en cryptographie). Equations, loi de groupe, coordonnées affines et projective. Courbes sur un corps fini, théorème de Hasse, comptage des points (élémentaire) par la loi de réciprocité quadratique. La méthode ECM de Lenstra, importance de la méthode de Montgomery. Test ECPP d'Atkin-Morain (notions de multiplication complexe). Utilisation du log discret en cryptographie.

(5) Cryptographie à clef publique (chiffrement et signature). Méthode RSA, problème de la taille de la clef, vulnérabilité à certaines attaques (necessité de padding et de hashing). Echange de clef bipartite de Diffie-Hellman. Méthode de chiffrement, et de signature El Gamal.

(6) Calcul d'un logarithme discret : méthode de Pohlig-Hellman (necessité d'un cardinal ayant un gros facteur premier), méthodes génériques d'attaque (Baby Step Giant Step de Shanks, Pollard rho à nouveau, le théorème de Shoup). Méthodes particulières pour certains groupes (index calculus, descente de Weil).