DAFTAR ISTILAH

Cryptography : Ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data.

Avalanche Effect : Nilai yang digunakan untuk menentukan baik atau tidaknya suatu algoritma.

Plaintext : Pesan asli sebelum dilakukan proses enkripsi.

Chipertext : Pesan hasil proses enkripsi.

Cryptanalyst : Orang yang ahli dalam menganalisis dan memecahkan kode dan chipper.

Key : biasanya terdiri dari karakter string singkat yang bersifat rahasia, yang dibutuhkan untuk mendeskripsi teks sandi.

Pseudo Random Generator : pembangkit rangkaian bilangan pseudo random, dimana proses pembangkitan tiap elemen tergantung dari formulasi matematis yang digunakan.

Seed : input yang digunakan pada pseudo random bit generator , sedangkan outputnya disebut pseudo random bit sequences (rangkaian bit semi acak). *Padding* : penambahan bit-bit dummies untuk menggenapi menjadi panjang blok yang sesuai, biasanya dilakukan pada blok terakhir *plaintext*.

Stream chipper : algoritma sandi yang mengenkripsi data persatuan data, seperti bit, byte, nible, atau per lima bit (saat data yang di enkripsi berupa data Boudout), setiap mengenkripsi satuan data digunakan kunci yang merupakan hasil pembangkitan dari kunci sebelum.

Block chipper : skema algoritma sandi yang akan mebagi-bagi teks yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan

	panjang t, dan setiap blok dienkripsi dengan menggunakan kunci yang sama.
AES	: Advance Encryption Standard. Suatu kompetisi untuk menetapkan metode enkripsi standar di Amerika.