Daftar Istilah

Advanced Encryption Standard (AES), algoritma enkripsi standard untuk penyandian data yang disahkan oleh NIST, berlaku mulai tahun 2001.

Avallanche Effect, analisa berapa besar perubahan pada bit-bit ciphertext akibat perubahan satu bit pada plaintext.

Brute Force Attack, merupakan suatu metoda memecahkan dengan cara mencoba semua variasi kunci yang mungkin.

Ciphertext, bentuk data teracak hasil dari proses enkripsi.

Cryptanalysis, seni dan ilmu untuk memecahkan ciphertext menjadi plaintext tanpa melalui cara yang seharusnya (dekripsi).

Cryptography/Kriptografi, ilmu tentang cara-cara menyandikan pesan yang bertujuan untuk menghindari perolehan pesan secara tidak sah.

Hash Function, merupakan fungsi pengacak dimana input kunci user dengan panjang bervariasi akan diacak menjadi suatu input kunci proses dengan ukuran yang tetap, sesuai dengan ukuran kunci algoritma enkripsi.

Initial Vektor (IV), block data tambahan untuk diproses pada mode operasi CBC, OFB, dan CFB.

National Institute of Standard Technology (NIST), merupakan badan pemerintah Amerika Serikat yang menetapkan standard suatu teknologi.

Plaintext, bentuk data asli sebelum proses enkripsi.

Private Key, merupakan kunci yang hanya memiliki oleh user untuk digunakan pada proses kriptografi asimetris.

Public Key, merupakan kunci public yang dimiliki dan diketahui oleh banyak orang untuk proses kriptografi asimetris.

Semi Weak Key (Kunci Setengah Lemah), merupakan suatu pasang kunci dimana bila plaintext dienkripsi dengan suatu semi weak key dan dienkripsi lagi dengan pasangan semi weak key-nya akan menghasilkan plaintext kembali.

Weak Key (Kunci Lemah), merupakan suatu kunci dimana bila plaintext dienkripsi dengan weak key dan ciphertext hasil enkripsi dienkripsi lagi dengan weak key, akan menghasilkan plaintext semula.