Nama Kelompok : - Sandi Prayogo (2018510)
- Nanda Bagoes Kurniawan (2018510)
- Andi Muhammad Galih (2018510)
- Andika Eka Saputra (2018510)

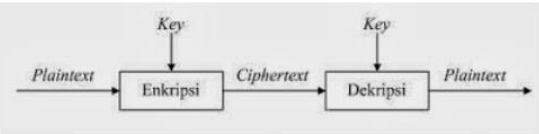
PENGERTIAN DAN SEJARAH KRIPTOGRAFI

Kriptografi adalah Secara etimologi kata kriptografi (*Cryptography*) berasal dari bahasa Yunani, yaitu kryptos yang artinya yang tersembunyi dan graphein yang artinya tulisan (Prayudi, 2005). Awal mula kriptografi dipahami sebagai ilmu tentang menyembunyikan pesan (Sadikin, 2012), tetapi seiring perkembangan zaman hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi (Diffie, 1976).

Istilah-istilah dalam Kriptografi

Dalam kriptografi akan dijumpai beberapa istilah-istilah penting antara lain adalah plaintext, ciphertext, enkripsi, dekripsi, cryptanalysis, dan cryptology. Plaintext adalah data yang dapat dibaca, sedangkan teknik untuk menjadikan data tidak dapat dibaca disebut enkripsi. Data yang telah dienkripsi disebut ciphertext, dan teknik untuk mengembalikan ciphertext menjadi plaintext disebut dekripsi (Prayudi, 2005). Cipher merupakan algoritma kriptografi, yakni fungsi matematika yang berperan dalam enkripsi dan dekripsi data (Rizal, 2011). Pelaku yang ahli dalam bidang kriptografi disebut cryptographer.

Cryptanalysis adalah ilmu untuk memecahkan ciphertext menjadi plaintext dengan tidak melalui cara yang semestinya, sedangkan orang yang menguasai ilmu ini disebut Cryptanalyst. Cabang matematika yang meliputi kriptografi dan cryptanalysis disebut Cryptology, sedangkan orang yang menguasai ilmu ini disebut cryptologist.



Proses enkripsi dan dekripsi

Jenis Kriptografi Berdasarkan Perkembangan

Algoritma kriptografi dapat diklasifikasikan menjadi menjadi dua jenis berdasarkan perkembangannya, yaitu kriptografi klasik dan kriptografi modern.

a. Algoritma Kriptografi Klasik

Algoritma ini digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya (Sadikin, 2012). Teknik substitusi adalah menggantikan karakter dalam plaintext menjadi karakter lain yang hasilnya adalah ciphertext. Sedangkan transposisi adalah teknik mengubah plaintext menjadi ciphertext dengan cara permutasi karakter. Kombinasi keduanya secara kompleks adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern (Prayudi, 2005).

b. Algoritma Kriptografi Modern

Algoritma ini memiliki tingkat kesulitan yang kompleks (Prayudi, 2005), dan kekuatan kriptografinya ada pada key atau kuncinya (Wirdasari, 2008). Algoritma ini menggunakan pengolahan simbol biner karena berjalan mengikuti operasi komputer digital. Sehingga membutuhkan dasar berupa pengetahuan terhadap matematika untuk menguasainya (Sadikin, 2012).

Jenis Kriptografi Berdasarkan Kunci

Algoritma kriptografi dapat diklasifikasikan menjadi dua jenis berdasarkan kuncinya, yaitu algoritma simetris dan algoritma asimetris (Prayudi, 2005).

a. Algoritma Simetris

Algoritma ini disebut simetris karena memiliki key atau kunci yang sama dalam proses enkripsi dan dekripsi sehingga algoritma ini juga sering disebut algoritma kunci tunggal atau algoritma satu kunci. Key dalam algoritma ini bersifat rahasia atau private key sehingga algoritma ini juga disebut dengan algoritma kunci rahasia (Prayudi, 2005).

b. Algoritma Asimetris

Algoritma ini disebut asimetris karena kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi. Kunci yang digunakan untuk enkripsi adalah kunci publik atau public key sehingga algoritma ini juga disebut dengan algoritma kunci publik. Sedangkan kunci untuk dekripsi menggunakan kunci rahasia atau private key (Prayudi, 2005)

Sejarah Kriptografi

Sejarah penulisan rahasia tertua dapat ditemukan pada peradaban Mesir kuno, yakni tahun 3000 SM. Bangsa Mesir menggunakan ukiran rahasia yang disebut dengan *hieroglyphics* untuk menyampaikan pesan kepada orang-orang yang berhak.

Awal tahun 400 SM bangsa Spartan di Yunani memanfaatkan kriptografi di bidang militer dengan menggunakan alat yang disebut *scytale*, yakni pita panjang berbahan daun papyrus yang dibaca dengan cara digulungkan ke sebatang silinder. Sedangkan peradaban Cina dan Jepang menemukan kriptografi pada abad 15 M.

Scytale

Peradaban Islam juga menemukan kriptografi karena penguasaannya terhadap matematika, statistik, dan linguistik. Bahkan teknik kriptanalisis dipaparkan untuk pertama kalinya pada abad 9 M oleh seorang ilmuwan bernama Abu Yusuf Ya'qub ibn 'Ishaq as-Shabbah al Kindi atau dikenal dengan Al-Kindi yang menulis kitab tentang seni memecahkan kode. Kitabnya berjudul ***Risalah fi Istikhraj al-Mu'amma*** (Manuskrip untuk memecahkan pesan-pesan Kriptografi). Terinspirasi dari perulangan huruf dalam Al-Qur'an, Al-Kindi menemukan teknik analisis frekuensi, yakni teknik untuk memecahkan ciphertext berdasarkan frekuensi kemunculan karakter pada sebuah pesan (Wirdasari, 2008)

Risalah fi Istikhraj al-Mu'amma