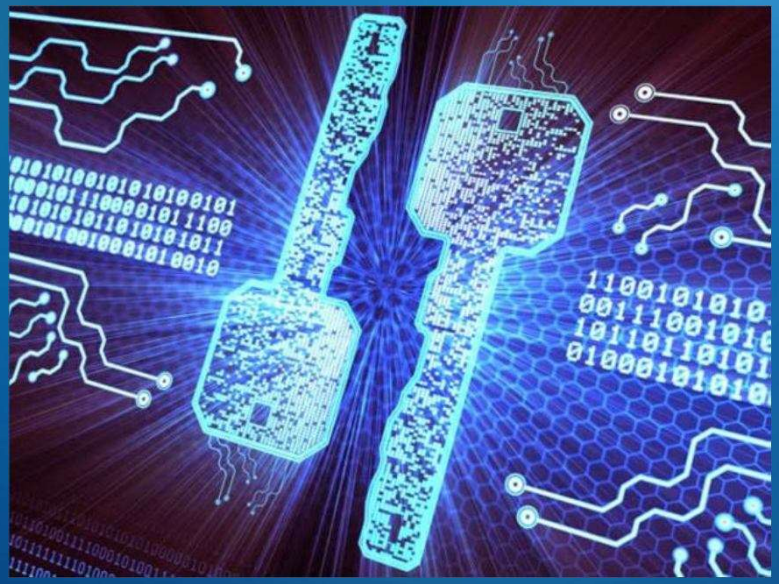
Pendahuluan

Kriptografi berasal berasal dari bahasa Yunani yaitu crypto berarti rahasia (secret) dan graphia berarti tulisan (writing). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika dikirim.



Pendahuluan

Sejarah Kriptografi

Sejak 4000 tahun lalu kriptografi telah dikenal oleh orang-orang Mesir lewathieroglyph walaupun bukan dalam bentuk tulisan standard. Pada zaman Rumawi Kuno, Julius Caesar mengirimkan pesan rahasia kepada panglima perang di medan perang dengan mengganti semua susunan alfabet dari: a b c d e f g h i j k l m n o p q r s t u v w x y z, menjadi: d e f g h i j k l m n o p q r s t u v w x y z a b c.

Pendahuluan

Pada zaman Rumawi Kuno, telah ada alat untuk mengirim pesan rahasia dengan nama Scytale yang digunakan oleh tentara Sparta. Scytale merupakan alat yang memiliki pita panjang dari daun papirus dan sebatang silinder. Pesan ditulis diatas pita yang dililitkan pada sebatang silinder, setelah itu pita dilepas dari batang silinder lalu dikirim. Untuk membaca pesan, pita tersebut dililitkan kembali pada sebatang silinder yang diameternya sama sehingga yang menjadi kunci pada Scytale adalah diameter silinder.

Pendahuluan

Perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Antar kota antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Pendahuluan

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah

kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Pendahuluan

Algoritma kriptografi berdasarkan jenis kunci yang digunakan dapat dibedakan menjadi dua jenis yaitu :

- Algoritma Simetri (Kriptografi Klasik)

Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi adalah kunci yang sama

- Algoritma Asimetri (Kriptografi Publik)

Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.

Pendahuluan

3. Konsep Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga pesan (informasi) agar tetap aman (secure).

Pendahuluan

Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

- Confidelity (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.

Pendahuluan

- Data integrity (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
- Authentication (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
- Non-repudiation (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk
- menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Pendahuluan

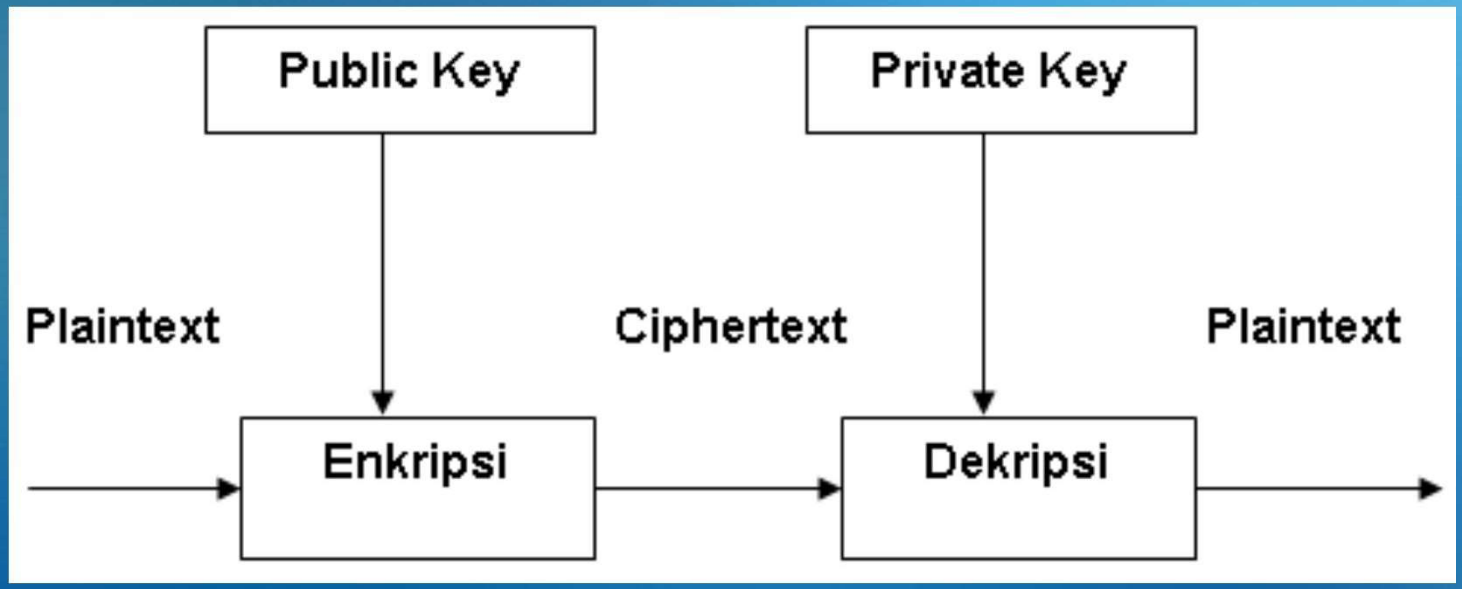
- Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

Pendahuluan

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

- Plaintext (M) adalah pesan yang hendak dikirimkan (berisi data asli).
- Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
- Enkripsi (fungsi E) adalah proses pengubahan plaintext menjadi ciphertext.
- Dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal/asli.
- Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Pendahuluan



Pendahuluan

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (plaintext) ke dalam bentuk data sandi (ciphertext) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (sender) kepada penerima (receiver). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali.

Proses tranformasi dari plaintext menjadi ciphertext disebut proses Enciphermentatau enkripsi

(encryption), sedangkan proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (decryption).

Pendahuluan

Untuk mengenkripsi dan mendekripsi data. Kriptografi menggunakan suatu algoritma (cipher) dan kunci (key). Cipher adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi data. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.

Pendahuluan

Algoritma kriptografi adalah algoritma yang berfungsi untuk melakukan tujuan dari ilmu kriptografi itu sendiri. Algoritma kriptografi terdiri dari 2 bagian fungsi, yaitu :

1. ENKRIPSI (encryption)

Proses tranformasi dari plaintext menjadi ciphertext disebut prosesEncipherment atau enkripsi (encryption).

2. DEKRIPSI (decryption).

Proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (decryption).

CRYPTOSYSTEM

Cryptographic system atau cryptosystem adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi.

CRYPTOSYSTEM

Kriptografi dapat memenuhi kebutuhan umum suatu transaksi:

1. Kerahasiaan (confidentiality) dijamin dengan melakukan enkripsi (penyandian).
2. Keutuhan (integrity) atas data-data pembayaran dilakukan dengan fungsi hash satu arah.
3. Jaminan atas identitas dan keabsahan (authenticity) pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan password atau sertifikat digital. Sedangkan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital.
4. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (non-repudiation) dengan memanfaatkan tanda tangan digital dan sertifikat digital.

CRYPTOSYSTEM

Karakteristik cryptosytem yang baik sebagai berikut:

1. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
2. Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
3. Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
4. Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya

CRYPTOSYSTEM

JENIS PENYERANGAN PADA PROTOKOL

- Ciphertext-only attack. Dalam penyerangan ini, seorang cryptanalyst memiliki ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.
- Known-plaintext attack. Dalam tipe penyerangan ini, cryptanalyst memiliki akses tidak hanya ke ciphertext sejumlah pesan, namun ia juga memiliki plaintext pesan-pesan tersebut.
- Chosen-plaintext attack. Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.

CRYPTOSYSTEM

JENIS PENYERANGAN PADA PROTOKOL

- Ciphertext-only attack. Dalam penyerangan ini, seorang cryptanalyst memiliki ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.
- Known-plaintext attack. Dalam tipe penyerangan ini, cryptanalyst memiliki akses tidak hanya ke ciphertext sejumlah pesan, namun ia juga memiliki plaintext pesan-pesan tersebut.
- Chosen-plaintext attack. Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.

Contoh

index.php:

```
<html>
<head>
<title>Program Enkripsi</title>
</head>
<body>
<h1>Program Enkripsi dengan php</h1>
<form action="proses.php" method="POST">
<table cellpadding="4">
<tr>
```

Contoh

```
<select name="enkripsi">
<option value="pilih">- Pilih Enkripsi -</option>
<option value="a">Dibalik</option>
<option value="b">ASCII</option>
<option value="c">Tukar Huruf</option>
<option value="d">Base64</option>
</select></td>
</tr>
<tr>
</table><br><br>
<input type="submit" value="Proses">
```

Contoh

```
<input type="reset" value="Reset">
<br><br><br><br>
</form>
</body>
</html>
```

Contoh

Hasil:

Daftar Pustaka

- Sitorus Lamhot, Algoritma dan Pemrograman, Andi, 2010

- Febriana Henny, Perdana Agus, Sulistianingsih Indri, Belajar algoritma dan pemrograman C++, Deepublish, 2010.