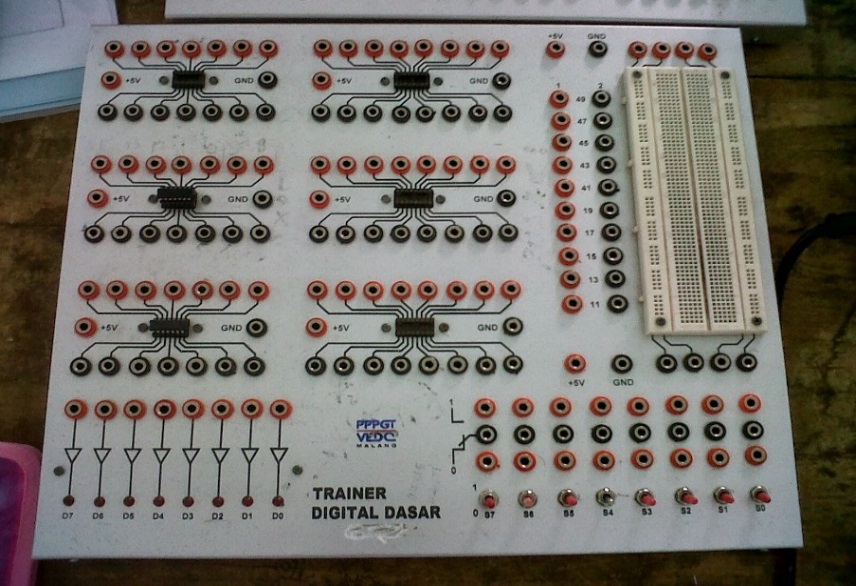
# **BAB 8**

# **FUNGSI DALAM KRIPTOGRAFI**



Data menjadi sesuatu yang amat berharga di dalam abad teknologi informasi saat ini. Perlakuan khusus terhadap data diperlukan apabila data ditujukan hanya untuk kalangan terbatas.Salah satu bidang ilmu yang dapat dipakai untuk membantu melakukan perlakuan khusus tersebut adalah menggunakan Kriptografi

1. Mahasiswa mampu memamahi definsi kruptografi dan tujuannya!
2. Mahasiswa mampu memberikan contoh-contoh penggunaan kriptografi dalam kehidupan sehari-hari
3. Mahasiswa memahami langkah-langkah untuk melakuan enkripsi dengan menggunakan Vigènere Cipher
4. Mahasiswa mampu membuat enkripsi dari sebuah atau lebih kata yang telah diketahui kuncinya
5. Mahasiswa mampu memecahkan sandi (deskripsi) dari sebuah atau lebih sandi jika dikethui kuncinya

**Tujuan Instruksional**

**Umum**

## **Pendahuluan**

Kriptografi  adalah  bidang  ilmu pengetahuan  yang  mempelajari  pemakaian persamaan  matematika  untuk  melakukan  proses penyandian data. Kriptografi bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut.

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu:

1. Kerahasiaan (confidentiality) adalah layanan yang digunakan untuk menjaga isi informasi dari semua pihak kecuali pihak yang memiliki otoritas terhadap informasi. Ada beberapa pendekatan untuk menjaga kerahasiaan, dari pengamanan secara fisik hingga penggunaan algoritma matematika yang membuat data tidak dapat dipahami. Istilah lain yang senada dengan confidentiality adalah secrecy dan privacy.
2. Integritas data adalah layanan penjagaan pengubahan data dari pihak yang tidak berwenang. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam pesan yang sebenarnya. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (digital signature). Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli.
3. Otentikasi adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication atau entity authentication) maupun mengidentifikasi kebenaran sumber pesan (data origin authentication). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi asalnya. Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (digital signature). Tanda-tangan digital menyatakan sumber pesan.
4. Nirpenyangkalan (non-repudiation) adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan Non-repudiasi, adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

Beberapa contoh dalam kehidupan yang menggunakan kriptografi

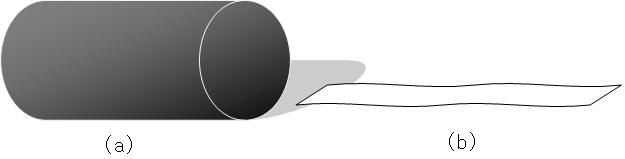
1. Komunikasi dengan Telepon Seluler
2. Pay TV
3. Transaksi lewat Anjungan Tunai mandiri (ATM)
4. Transaksi e-commerce via ineternet



Gambar 1 Orang yang sedang bertransaksi di mesin ATM

## **Sejarah Kriptografi**

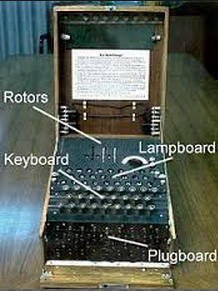
Kriptografi sudah digunakan 4000 tahun yang lalu yang dipekenalkan oleh orang-orang Mesir untuk mengirim pesan ke pasukan militer yang berada dilapangan dan supaya pesan tersebut tidak terbaca oleh pihak musuh walaupun kurir pembawa pesan tersebut tertangkap oleh musuh. Bangsa Sparta, suatu bangsa militer pada jaman Yunani kuno, menggunakan teknik kriptografi yang disebut scytale, untuk kepentingan perang. Scytale terbuat dari tongkat dengan papyrus yang mengelilinginya secara spiral. Kunci dari scytale adalah diameter tongkat yang digunakan oleh pengirim harus sama dengan diameter tongkat yang dimiliki oleh penerima pesan, sehingga pesan yang disembunyikan dalam papyrus dapat dibaca dan dimengerti oleh penerima.



(a) Silider, yang digunakan untuk melilitkan pita pesan (b) Pita pesan bisa berupa kain atau kertas yang bisa dililitkan di siliner

Julius Caesar, seorang kaisar terkenal Romawi yang menaklukkan banyak bangsa di Eropa dan Timur Tengah juga menggunakan suatu teknik kriptografi yang sekarang disebut Caesar cipher untuk berkorespondensi sekitar tahun 60 S.M. Teknik yang digunakan oleh Sang Caesar adalah mensubstitusikan alfabet secara beraturan, yaitu oleh alfabet ketiga yang mengikutinya, misalnya, alfabet ‘’A" digantikan oleh "D", "B" oleh "E", dan seterusnya.

Pada Perang Dunia ke II, Pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan Enigma. Mesin yang menggunakan beberapa buah rotor (roda berputar) ini melakukan enkripsi dengan cara yang sangat rumit. Namun Enigma cipher berhasil dipecahkan oleh pihak Sekutu dan keberhasilan memecahkan Enigma sering dikatakan sebagai faktor yang memperpendek perang dunia ke-2.



Gambar Mesin Enigma

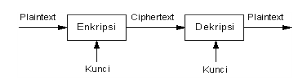
(Sumber : wikipedia)

## **Terminologi Dalam Kriptografi**

Di dalam kriptografi kita akan sering menemukan berbagai istilah atau terminologi. Beberapa istilah yang penting untuk diketahui adalah sebagai berikut.

1. **Plainteks** (*plaintext* atau *cleartext*, artinya teks jelas yang dapat dimengerti): pesan yang dirahasiakan. Pesan dapat berupa data atau informasi yang dikirim atau yang disimpan di dalam media perekaman (kertas, storage, dan sebagainya). Pesan yang tersimpan tidak hanya berupa teks, tetapi juga dapat berbentuk citra (image), suara/bunyi (audio), dan video, atau berkas biner lainnya.
2. **Chiperteks** (*chipertext* atau *cryptogram*, artinya teks tersandi), Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami (enkripsi).
3. **Enkripsi** (*encryption* atau *enchipering*): proses penyandian dari plainteks ke chiperteks.
4. **Dekripsi** (*decryption* atau *dechipering*): proses pembalikan dari chiperteks ke plainteks
5. **Algoritma kriptografi** (atau *chiper*): aturan untuk *enchipering* dan *dechipering* atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi.
6. **Kriptografer**: orang menggunakan algoritma kriptografi untuk merahasiakan pesan dan mendekripsikannya kembali
7. **Kriptanalisis** (*cryptanalysis*): ilmu dan seni untuk memecahkan chiperteks, berupa proses untuk memperoleh plainteks dari chiperteks tanpa mengetahui *kunci* yang diberikan. Pelakunya disebut **kriptanalis**.
8. **Kriptologi** (*cryptology*): studi mengenai kriptografi dan kriptanalisis. Kriptologi dapat juga diartikan sebagai seni dan ilmu untuk membuat dan memecahkan kode rahasia.

Secara sederhana istilah-istilah diatas dapat digambarkan sebagai berikut :



Gambar Proses Enkripsi/Dekripsi Sederhana

Lahir dengan nama asli Marian Adam Rejewski di Bromberg, sekarang Bydgoszcz, 16 Agustus 1905. Ia adalah matematikawan dan kriptolog Polandia yang pada tahun 1932 berhasil memecahkan kode deskripsi mesin enigma, mesin penyandi utama yang digunakan oleh bangsa Germany. Keberhasilan Rejewski dan rekan kerjanya Jerzy Różycki dan Henryk Zygalski membuat negara Britania Raya yang pertama kali membaca enigma pada Perang Dunia II.

**Tokoh**



## **Jenis – Jenis Kriptografi**

Dalam kriptografi, sistem penyandian dapat dikelompokan menjadi 2 kelompok, yaitu sistem cipher klasik dan sistem cipher modern.

1. Sistem cipher klasik

Sistem algoritma kriptografi yang digunakan pada zaman dahulu yang masih berbasis karakter sehingga algoritmanya tidak terlalu sulit untuk dipecahkan. Sitem ciper kalsik termasuk ke dalam kriptografi kunci-simetri. Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi ini melakukan pengacakan huruf pada kata terang / plaintext. Kriptografi ini hanya melakukan pengacakan pada huruf A - Z, dan sangatlah tidak disarankan untuk mengamankan informasi-informasi penting karena dapat dipecahkan dalam waktu singkat. Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern. Tiga alasan mempelajari algoritma klasik:

* 1. Memahami konsep dasar kriptografi.
  2. Dasar algoritma kriptografi modern.
  3. Memahami kelemahan sistem cipher.

1. Sistem cipher modern

Sistem algoritma yang sampai saat ini masih digunakan karena berbasis bit sehingga cukup sulit untuk dipecahkan dan tingkat keamanannya lebih tinggi dibandingkan dengan sistem cipher klasik. Salah satu cipher modern yang ada saat ini adalah kriptografi kunci public Kriptografi kunci publik mengacu pada system kriptogafi yang memerlukan dua kunci yang berbeda, satu untuk mengunci atau mengenkripsi plaintext, dan satu lagi untuk membuka atau mendekripsi cyphertext. Setiap kunci hanya bisa melakukan salah satu fungsi saja. Salah satu kunci akan disebarkan, yang disebut public key, sedangkan kunci yang satunya akan dirahasiakan atau disebut private key.

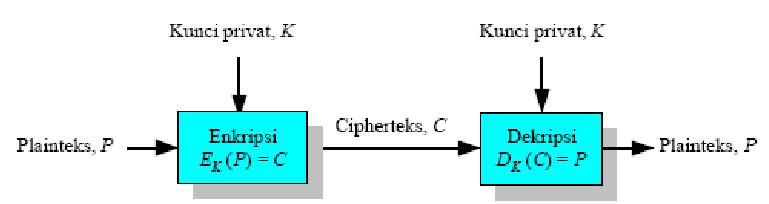
Kriptografi kunci publik menggunakan algoritma kunci asimetrik, yang lebih dikenal sebagai asymmetric key cryptography. Algoritma tersebut memiliki property public key dan private key dimana salah satu kunci tidak memiliki informasi dari kunci lainnya. Public key digunakan untuk mengubah suatu pesan menjadi bentuk yang tidak dapat dibaca dan dapat didekripsi menggunakan private key yang cocok.

## **Algoritma Kriptografi**

Algoritma menggambarkan sebuah prosedur komputasi yang terdiri dari variabel input dan menghasilkan output yang berhubungan. Algoritma kriptografi atau sering disebut dengan cipher adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Algoritma kriptografi ini bekerja dalam kombinasi dengan menggunakan kunci (key) seperti kata, nomor atau frase tertentu. Berdasarkan kunci yang dipakai, algoritma kriptografi dapat dibedakan atas dua jenis yaitu algoritma simetrik (symmetric) dan asimetrik (asymmetric).

1. Algoritma Simetrik

Algoritma simetrik dapat pula disebut sebagai algoritma konvensional. Algoritma simetris (*symmetric algorithm*) adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm*. Algoritma simetri merupakan satu-satunya algoritma kriptografi yang dikenal dalam catatan sejarah hingga tahun 1976. Semua algoritma kriptografi klasik termasuk ke dalam sistem kriptografi simetrik. Kelebihan algoritma simetris ini adalah proses enkripsi dan deskripsinya yang jauh lebih cepat dibandingkan dengan algoritma asimetris. Sedangkan kelemahan algoritma ini adalah permasalahan distribusi kunci (key distribution). Seperti yang telah dibahas, proses enkripsi dan deskripsi menggunakan kunci yang sama. Sehingga muncul persoalan menjaga kerahasian kunci, yaitu pada saat pengiriman kunci pada media yang tidak aman seperti internet.



Gambar . Skema Kriptografi Simetrik

1. Algoritma Asimetrik

Algoritma Asimetrik (Asymmetric atau Public Key) adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi dimana kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun (diumumkan ke publik), sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan (rahasia). Kriptografi kunci-publik dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Setiap orang dapat memasukkan surat ke dalam kotak surat tersebut, tetapi hanya pemilik kotak yang dapat membuka kotak dan membaca surat di dalamnya karena ia yang memiliki kunci.

Proses komunikasi menggunakan asymmetric key algorithms dapat dianalogikan seperti berikut:

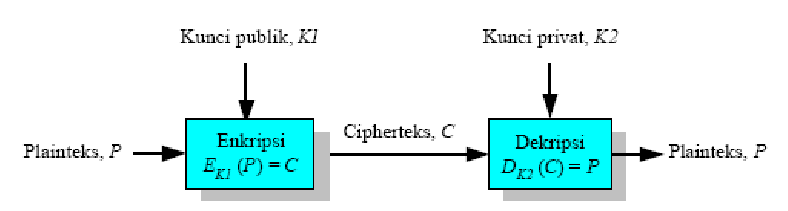
1. Hanung mengirim public key kepada Ferra melalui saluran yang tidak perlu aman.
2. Ferra mengirimkan ciphertext melalui saluran yang sama.
3. Robbi menyusup ke dalam komunikasi dan berhasil mendapatkan public key beserta ciphertext.
4. Hanung menerima ciphertext dan mendapatkan pesan dari Alice.

Contoh di atas menunjukkan meskipun Robbi berhasil mendapatkan public key beserta ciphertext, tetapi karena dia tidak mengetahui private key untuk mendekripsi ciphertext, hanya Hanung yang akan mengetahui isi pesan dari Ferra. Keuntungan dari kriptografi kunci publik antara lain adalah:

1. Tidak diperlukan pengiriman kunci rahasia
2. Jumlah kunci dapat ditekan

Sistem kriptografi kunci publik yang aman didasarkan pada fakta:

1. Komputasi untuk enkripsi/dekripsi pesan mudah dilakukan.
2. Secara komputasi hampir tidak mungkin menurunkan private key, bila diketahui public key pasangannya.



Gambar . Skema Kriptografi Asimetrik

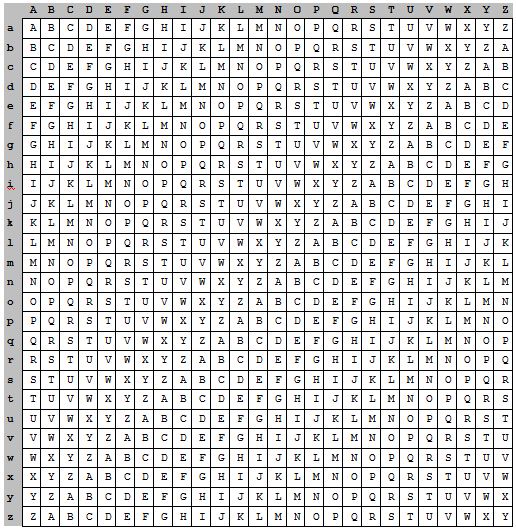
Untuk lebih memahami pengunaan kriptografi dalam kehidupan sehari – sehari , buka link berikut ini.

<http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Kriptografi%20dalam%20Kehidupan%20Sehari-hari%20(Bagian%201).pdf>

**Jendela Dunia**

## **Fungsi Modulo Dalam Kriptografi**

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Algoritma Vigenere Cipher ini menggunakan bujursangkar Vigenere untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf ciphertext yang diperoleh dengan Caesar cipher. Setiap kolom menunjukan kunci.



Gambar . Bujur Sangkar Vigenere

Vigenere chiper merupakan salah satu algoritma kriptografi klasik untuk menyandikan suatu plaintext dengan menggunakan teknik substitusi.Vigenere cipher pada dasarnya cukup rumit untuk dipecahkan. Meskipun begitu, Vigenere cipher tetap memiliki kelemahan. Salah satunya adalah dapat diketahui panjang kuncinya dengan menggunakan metode kasiski. Hal ini disebabkan karena umumnya terdapat frasa yang berulang-ulang pada ciphertext yang dihasilkan.

Jika diperhatikan dengan seksama, bujur sangkar Vigenere chipper dapat diperoleh dengan mengguanakan fungsi modulo dimana:

|  |
| --- |
| Plainteks = (P + K) Modulo 26 …………………… (1)  Chiper Teks = (C – K) Modulo 26 ……………….. (2) |

Dengan :

P = Indeks Plainteks

K = Indeks Kunci

C = Indeks chiperteks

Yang diperoleh dari table berikut

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Huruf | A | B | C | D | E | F | G | H | I | J | K | L | M |
| Indeks | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Huruf | O | P | Q | R | S | T | U | V | W | X | Y | Z |  |
| Indeks | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 25 |  |

**Contoh :**

Buatlah sandi (enkripsi) dengan dari kata POLTEK dengan Kunci HRO menggunakan Vigènere Cipher!

**Solusi:**

* Dari tiap-tiap huruf di plaintext, kita pasangkan satu-satu secara berurutan dengan kuncinya, karena kuncinya cuma 3 karakter, sedangkan plaintextnya lebih dari itu, berarti kuncinya kita ulang hingga sesuai dengan panjang plaintextnya.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Plaintext** | **P** | **O** | **L** | **T** | **E** | **K** |
| **Kunci** | **H** | **R** | **O** | **H** | **R** | **O** |

* Proses berikutnya, kita ubah kunci nya jadi index hurufnya, yang nantinya akan kita tambahkan ke index plaintextnya (A=0, Z=25):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Plaintext** | **P** | **O** | **L** | **T** | **E** | **K** |
| **Index Plaintext** | 15 | 14 | 11 | 19 | 4 | 10 |
| **Kunci** | **H** | **R** | **O** | **H** | **R** | **O** |
| **Index Kunci** | 7 | 17 | 14 | 7 | 17 | 14 |
| **(Plaintext + Kunci) Mod 26** | 22 | 5 | 25 | 0 | 21 | 24 |
| **Ciphertext** | **W** | **F** | **Z** | **A** | **V** | **Y** |

Jadi, kata “enkripsi” dari POLTEK dengan kunci HRO adalah WHFZAVY

**Contoh :**

Pecahkan sandi (dekripsi) jika diketahui chiperteks WHFZAVY dan Kunci HRO menggunakan Vigènere Cipher!

**Solusi:**

* Dari tiap-tiap huruf di chipertext, kita pasangkan satu-satu secara berurutan dengan kuncinya, karena kuncinya cuma 3 karakter, sedangkan chipertextnya lebih dari itu, berarti kuncinya kita ulang hingga sesuai dengan panjang chipertextnya.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ciphertext** | **W** | **F** | **Z** | **A** | **V** | **Y** |
| **Kunci** | **H** | **R** | **O** | **H** | **R** | **O** |

* Proses berikutnya, kita ubah kunci nya jadi index hurufnya, yang nantinya akan kita kurangi ke index chipertextnya (A=0, Z=25):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ciphertext** | **W** | **F** | **Z** | **A** | **V** | **Y** |
| **Index Chipertext** | 22 | 5 | 25 | 0 | 21 | 24 |
| **Kunci** | **H** | **R** | **O** | **H** | **R** | **O** |
| **Index Kunci** | 7 | 17 | 14 | 7 | 17 | 14 |
| **(Chipertext - Kunci) Mod 26** | 15 | 14 | 11 | 19 | 4 | 10 |
| **Plaintext** | **P** | **O** | **L** | **T** | **E** | **K** |

Jadi, dekripsi dari dari WHFZAVY dengan kunci HRO adalah POLTEK.

## **Ringkasan**

* Kriptografi adalah bidang ilmu pengetahuan yang mempelajari pemakaian persamaan matematika untuk melakukan proses penyandian data
* Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu karahasiaan, integritas data, otemtikasi, dan nirpenyangkalan
* Sistem penyandian dapat dikelompokan menjadi 2 kelompok, yaitu sistem cipher klasik dan sistem cipher modern.
* sistem cipher klasik adalah Sistem algoritma kriptografi yang digunakan pada zaman dahulu yang masih berbasis karakter
* sistem cipher modern adalah Sistem algoritma yang sampai saat ini masih digunakan karena berbasis bit sehingga cukup sulit untuk dipecahkan dan tingkat keamanannya lebih tinggi dibandingkan dengan sistem cipher klasik
* Algoritma kriptografi atau sering disebut dengan cipher adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi
* Berdasarkan kunci yang dipakai, algoritma kriptografi dapat dibedakan atas dua jenis yaitu algoritma simetrik (symmetric) dan asimetrik (asymmetric).
* Algoritma simetris (symmetric algorithm) adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi
* Algoritma Asimetrik (Asymmetric atau Public Key) adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi
* Fungsi modulo dimanfaatkan dalam proses enkripsi dan deskripsi pada kriptografi.

1. Sebutkan tahap-tahap menggunkan Algoritma kriptografi klasik Vigènere Cipher untuk mengubah sebuah Plainteks 🡪 Cipherteks 🡪 Plainteks!
2. Buatlah sandi (enkripsi) dengan dari kata berikut dengan sandi yang telah di tentukan dengan menggunakan Vigènere Cipher!
3. MATEMATIKA dengan Kunci DISKRIT
4. GREEN CAMPUS denga Kunci POLTEK!
5. POLITEKNIK TELKOM dengan Kunci AKU
6. Pecahkanlah kata sandi berikut ini denga menggunakan kunci POLTEK
7. ECWMIUISWDSW
8. VWGBRQPBOVEBXBR
9. HOMTVNJZFWSXV
10. IVPPSBAR
11. ECWMIUISWDSWVWGBRQPBOVEBXBRHOMTVNJZFWSXV

**Latihan Soal**

## **Daftar Pustaka**

|  |  |
| --- | --- |
| [1] | Onno W.P., Aang  Arif  Wahyudi,  2000,  Mengenal  eCommerce.  Elex Media Komputindo, Jakarta. |
| [2] | Ricky Gilbert Fernando, 2007, PENGGUNAAN FUNGSI HASH DALAM KRIPTOGRAFI, MAKALAH IF2153, Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika  Institut Teknologi Bandung |
| [3] | Dony Ariyus, Awal Sejarah Kriptografi di Dunia, Jurusan Teknik Informatika, STMIK AMIKOM Yogyakarta, Jl. Ring Road Utara, Condong Catur, Sleman, Yogyakarta - Indonesia |
| [4] | Tadya Rahanady Hidayat, 2011, Public Key Cryptography  Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung |
| [5] | Dafid, 2006, Kriptografi Kunci Simetris Dengan Menggunakan Algoritma Crypton. @lgortima Jurnal Ilmiah STMIK MDP Palembang Volume 2 Nomor 3 |
| [6] | Munir, Rinaldi. 2013. Matematika Diskrit. Bandung: Informatika |
| [7] | Rossen, Kenneth. 2011. Discrete Mathematics and Its Applications.7th.Edition. McGraw.Hill |
| [8] | Nugroho, H and Nindito H. 2012. Workbook Matematika Diskrit. Politeknik Telkom. |