Keamanan Sistem dan Jaringan

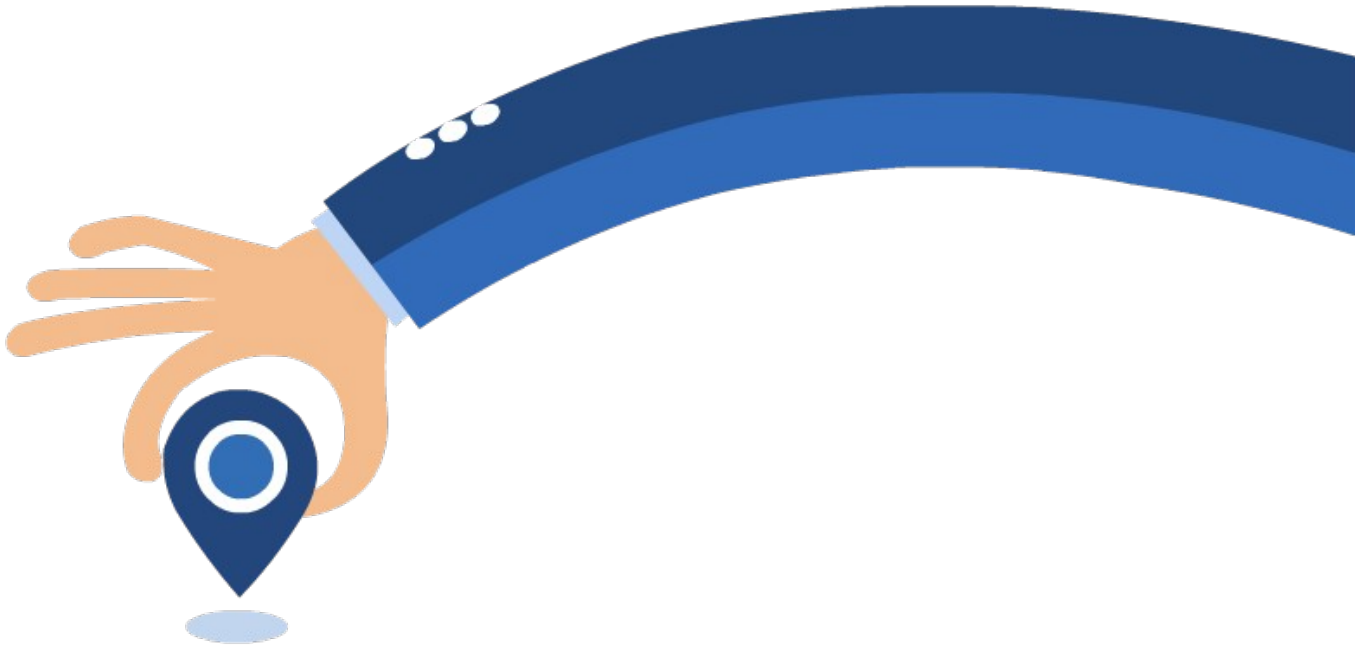
Pertemuan ke-4

Pesantren Teknologi Informasi dan Komunikasi
Jln. Mandor Basar No. 54 RT 01/RW 01 Rangkapanjaya,
Pancoran Mas, Depok 16435 | Telp. (021) 77 88 66 91
Koordinat (-6.386680 S, 106.777305 E)
www.petik.or.id

Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals



Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya, Pancoran Mas, Kota Depok 16435

www.petik.or.id 021 7788 6691 info@petik.or.id

Keamanan Data (Kriptografi)

Kriptografi

- Pengamanan dengan menggunakan kriptografi dilakukan dengan dua cara, yaitu **transposisi** dan **substitusi**
- Pada penggunaan transposisi, posisi dari huruf yang diubah-ubah, sementara pada substitusi, huruf (atau kata) digantikan dengan huruf atau simbol lain
- Jadi bedanya dengan steganografi adalah pada kriptografi pesan nampak. Hanya bentuknya yang sulit dikenali karena seperti diacak-acak

Kriptografi

- Kriptografi *(*cryptography*)* merupakan ilmu dan seni untuk menjaga pesan agar aman. *(Cryptography is the art and science of keeping messages secure)*
- *Crypto* berarti *secret* (rahasia) dan *graphy* berarti *writing* (tulisan)
- Para pelaku atau praktisi kriptografi disebut *cryptographers*.
- Sebuah algoritma kriptografik (*cryptographic algorithm*) disebut *cipher*, merupakan persamaan matematik yang digunakan untuk proses **enkripsi** dan **dekripsi**. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat

Kriptografi

- Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*). Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah *encipher*
- *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah

Kriptografi

- Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut dekripsi (*decryption*). Menurut ISO 7498-2, terminologi yang lebih tepat untuk proses ini adalah *decipher*
- *Cryptanalysis* adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci. *Cryptanalyst* adalah pelaku atau praktisi yang menjalankan *cryptanalysis*. *Cryptology* merupakan gabungan dari *cryptography* dan *cryptanalysis*

Kekuatan Algoritma

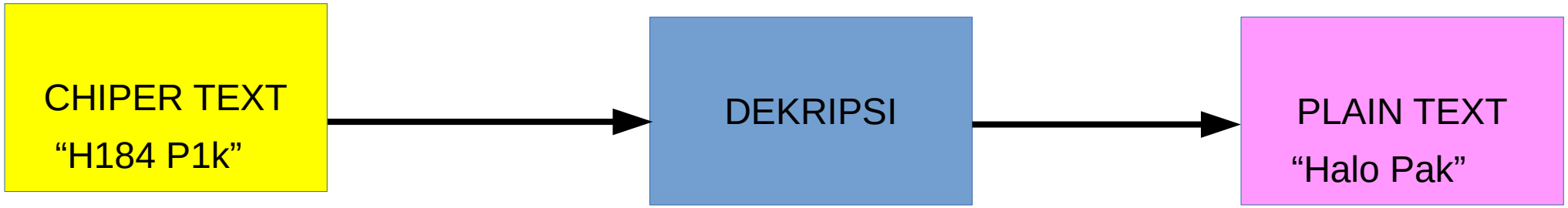
Sejumlah studi memperlihatkan bahwa di dunia nyata, kehandalan sebuah algoritma bukan terletak pada kerahasiaan algoritma itu sendiri, namun berada pada kuncinya. Secara prinsip algoritma yang dimaksud hanya melakukan dua proses transformasi, yaitu **enkripsi** dan **dekripsi**

Enkripsi

Enkripsi adalah proses transformasi mengubah teks terang (*plaintext)* menjadi teks sandi (*ciphertext*)

Dekripsi

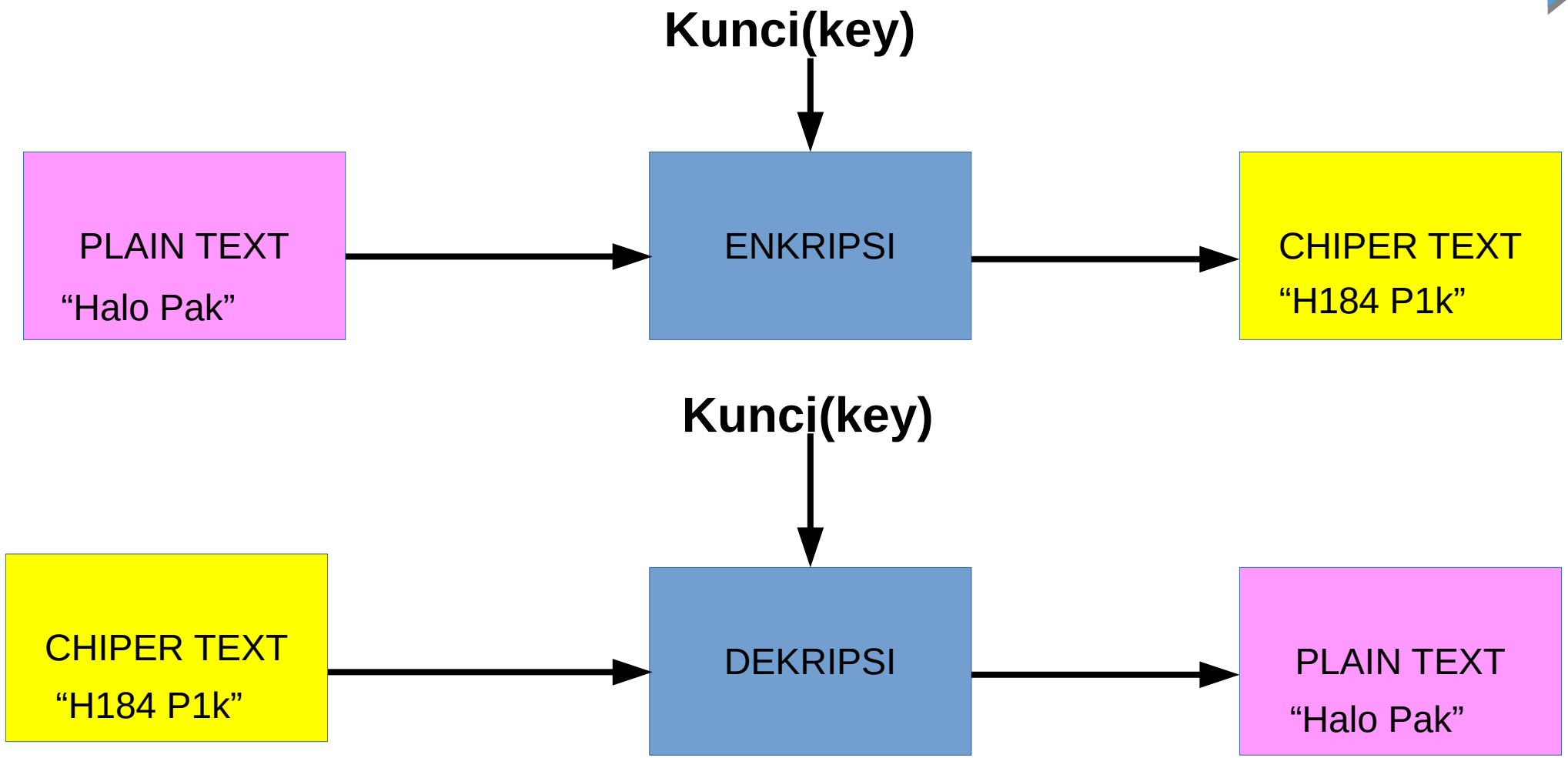
Dekripsi (proses transformasi sebaliknya dari enkripsi) adalah mengubah teks sandi menjadi teks terang



Kunci (*key*)

Adapun kunci yang dimaksud biasa dikenal sebagai istilah sederhana **password**, yang dalam implementasinya dapat berupa serangkaian campuran antara huruf, angka, dan simbol - hingga yang berbentuk biometrik seperti sidik jari, retina mata, karakter suara, suhu tubuh, dan berbagai kombinasi lainnya

Kunci


Kunci(key)
PLAIN TEXT
“Halo Pak”
ENKRIPSI
CHIPER TEXT
“H184 P1k”
Kunci(key)
CHIPER TEXT
“H184 P1k”
DEKRIPSI
PLAIN TEXT
“Halo Pak”

Kunci dan Panjang Kunci

- Kekuatan dari penyandian bergantung kepada kunci yang digunakan.
- Beberapa algoritma enkripsi memiliki kelemahan pada kunci yang digunakan. Untuk itu, kunci yang lemah tersebut tidak boleh digunakan.
- Selain itu, panjangnya kunci, yang biasanya dalam ukuran bit, juga menentukan kekuatan dari enkripsi.
- Kunci yang lebih panjang biasanya lebih aman dari kunci yang pendek.
- Jadi enkripsi dengan menggunakan kunci 128-bit lebih sukar dipecahkan dengan algoritma enkripsi yang sama tetapi dengan kunci 56-bit.

Algoritma Enkripsi

- Algoritma sandi kunci-simetris
  - Data Encryption Standard (DES)
  - Blowfish
  - Twofish
  - MARS
  - IDEA
  - 3DES
  - AES
- Algoritma sandi kunci-asimetris
  - Rivert-Shamir-Adelman (RSA)
  - Knapsack
  - Diffie-Heillman

Algoritma Hash

- MD5 (*Message-Digest Algorithm 5*)
- SHA (*Secure Hash Algorithm*)

Substitution Cipher

- Salah satu contoh dari *substitution cipher* adalah Caesar Cipher yang digunakan oleh Julius Caesar.
- Pada prinsipnya, setiap huruf digantikan dengan huruf yang berada tiga (3) posisi dalam urutan alfabet. Sebagai contoh huruf “a” digantikan dengan huruf “D” dan seterusnya. Transformasi yang digunakan adalah:

Plain: 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

Cipher: 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

Multiple-letter Encryption

Untuk meningkatkan keamanan, enkripsi dapat dilakukan dengan mengelompokkan beberapa huruf menjadi sebuah kesatuan (unit) yang kemudian dienkripsi. Ini disebut *multiple-letter encryption*. Salah satu contoh *multiple-letter encryption* adalah “Playfair”.

Playfair Cipher

- Teknik enkripsi simetris manual dan merupakan cipher substitusi digram literal pertama
- Skema ini ditemukan pada tahun 1854 oleh Charles Wheatstone
- Teknik ini mengenkripsi pasangan huruf (bigrams atau digram)

Teknik Playfair Cipher

- Playfair cipher menggunakan tabel 5x5 yang berisi kata kunci.
- Untuk membuat tabel kunci, pertama harus mengisi tabel dengan huruf-huruf dari kata kunci dengan menghilangkan huruf duplikat.
- Kemudian tabel diisi dengan sisa huruf-huruf alfabet dengan menempatkan huruf I dan J di tempat yang sama.
- Kata kunci dapat ditulis di baris atas tabel, dari kiri ke kanan atau dalam pola lain.

Teknik Playfair Cipher

- Untuk mengenkripsi pesan, teks dipecah menjadi digram (kelompok 2 huruf) misalnya, "HelloWorld" menjadi "HE LL OW OR LD".
- Digram ini akan diganti menggunakan tabel kunci.
- Karena enkripsi memerlukan pasangan huruf, pesan dengan jumlah karakter ganjil biasanya ditambahkan huruf yang tidak biasa, misalnya "X".
- Dua huruf digram dianggap berseberangan dengan persegi panjang di tabel kunci.

Teknik Playfair Cipher

- Untuk melakukan penggantian, terapkan 4 aturan berikut untuk setiap pasangan huruf dalam teks:
  - Jika kedua huruf sama (atau hanya satu huruf yang tersisa), tambahkan "X" setelah huruf pertama.
  - Jika huruf-huruf tersebut muncul di baris yang sama pada tabel, gantilah dengan huruf-huruf di sebelah kanannya
  - Jika huruf-huruf tersebut muncul di kolom yang sama pada tabel, gantilah dengan huruf-huruf tepat di bawahnya
  - Jika huruf-hurufnya tidak berada pada baris atau kolom yang sama, gantilah dengan huruf-huruf pada baris yang sama tetapi pada sudut-sudut yang bersebrangan.
  - Urutan itu penting - huruf pertama dari pasangan terenkripsi adalah yang terletak di baris yang sama dengan huruf pertama dari pasangan plaintext.

Contoh dengan gambar

- Asumsi akan mengenkripsi digram OR. Maka akan ada lima buah kasus, yaitu:

1)

*	*	*	*	*
*	0	Y	R	Z
*	*	*	*	*
*	*	*	*	*
*	*	*	*	*

Hence, OR -> YZ

2)

*	*	0	*	*
*	*	B	*	*
*	*	*	*	*
*	*	R	*	*
*	*	Y	*	*

Hence, OR -> BY

3)

Z	*	*	0	*
*	*	*	*	*
*	*	*	*	*
R	*	*	X	*
*	*	*	*	*

Hence, OR -> ZX

4)

*	*	*	*	*
*	*	*	*	*
*	0	R	C	*
*	*	*	*	*
*	*	*	*	*

Hence, OR -> RC

5)

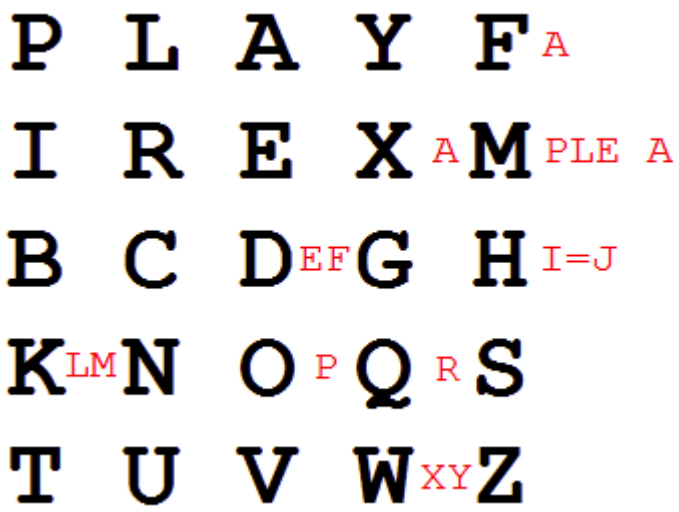
*	*	*	*	*
*	*	R	*	*
*	*	0	*	*
*	*	I	*	*
*	*	*	*	*

Hence, OR -> IO

Contoh Penggunaan

Akan mengenkripsi teks "Hide the gold in the tree stump"

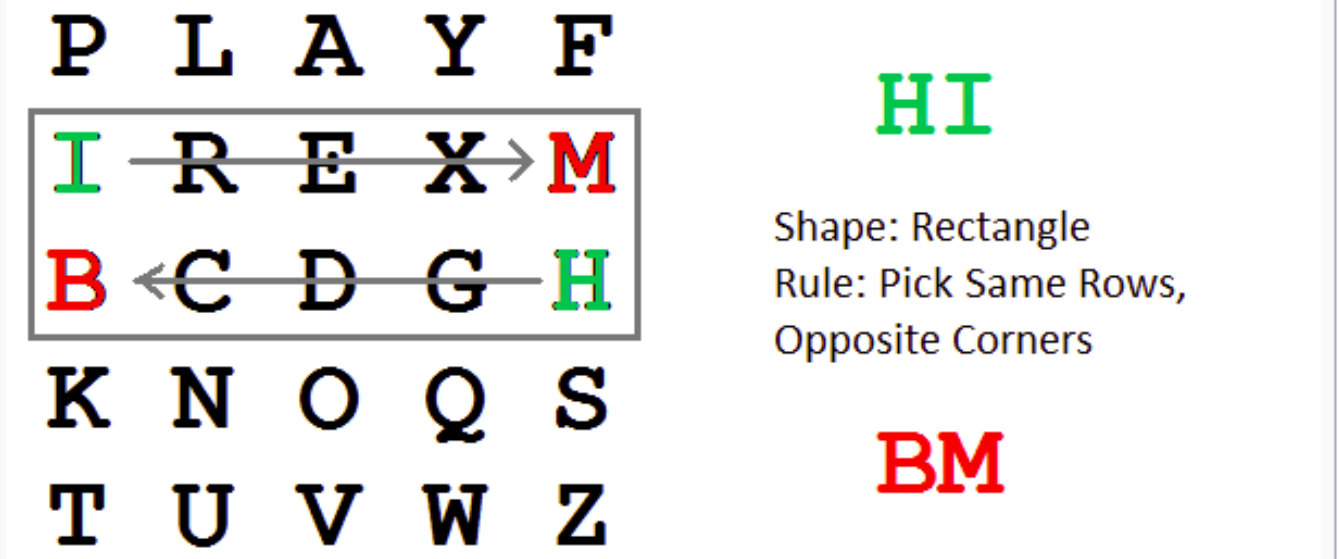
1. Buat table dengan kata kunci "playfair example"



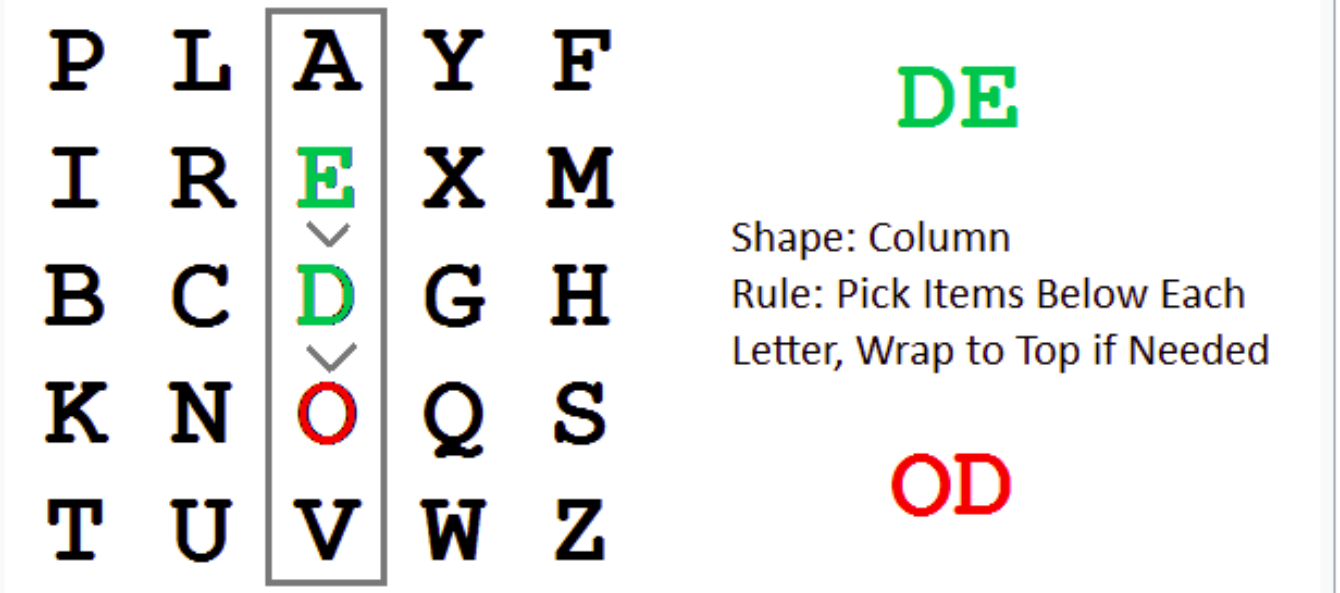
2. Buat pasangan huruf

   HI DE TH EG OL DI NT HE TR EX ES TU MP

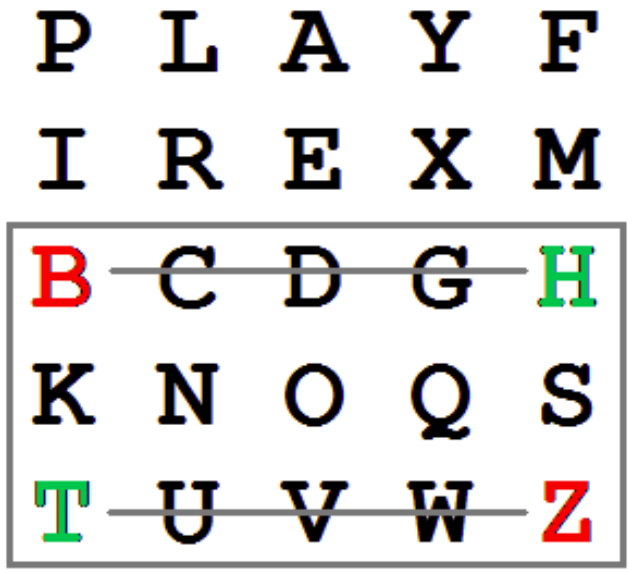
Proses Enkripsi

1. The pair HI forms a rectangle, replace it with BM	

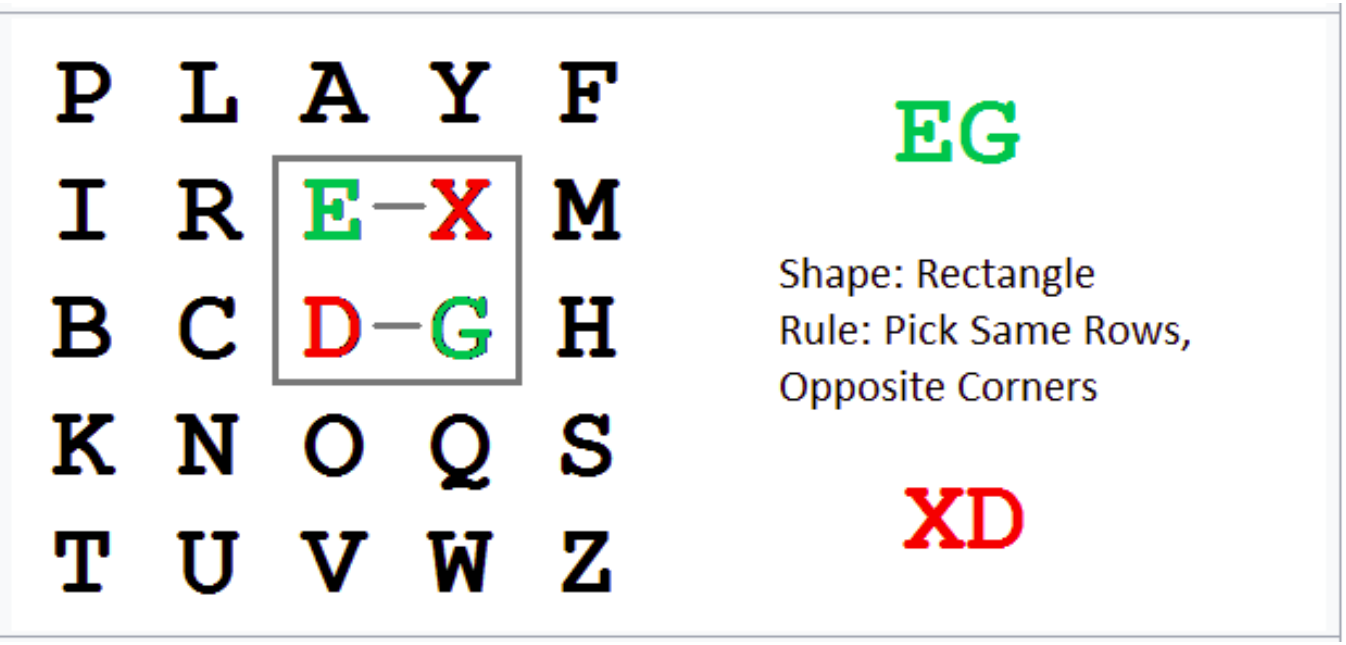
Proses Enkripsi

2. The pair DE is in a column, replace it with OD	

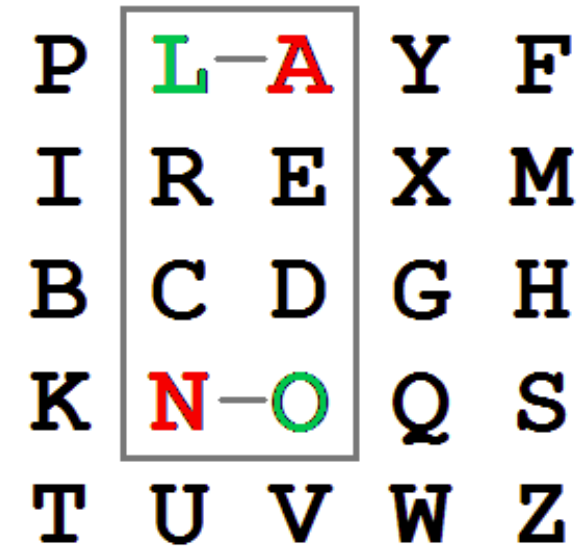
Proses Enkripsi

3. The pair TH forms a rectangle, replace it with ZB	

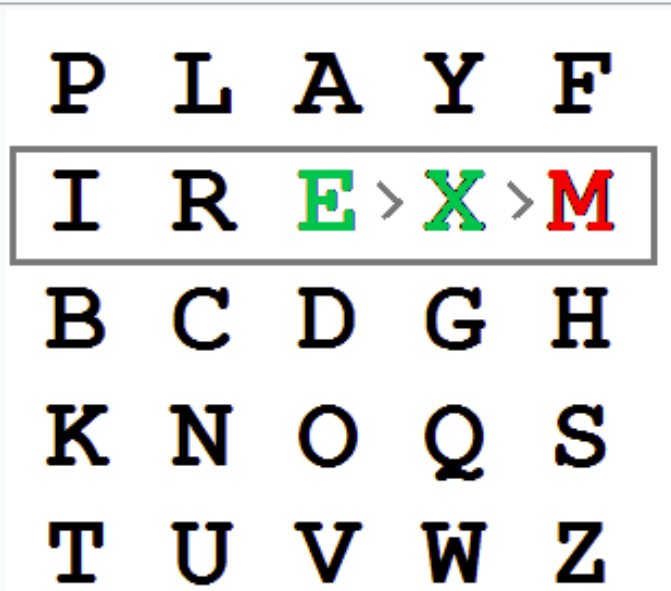
Proses Enkripsi

4. The pair EG forms a rectangle, replace it with XD	

Proses Enkripsi

5. The pair OL forms a rectangle, replace it with NA	 OL Shape: Rectangle Rule: Pick Same Rows, Opposite Corners NA
6. The pair DI forms a rectangle, replace it with BE	
7. The pair NT forms a rectangle, replace it with KU	
8. The pair HE forms a rectangle, replace it with DM	
9. The pair TR forms a rectangle, replace it with UI	

Proses Enkripsi

10. The pair EX (X inserted to split EE) is in a row, replace it with XM	
11. The pair ES forms a rectangle, replace it with MO	
12. The pair TU is in a row, replace it with UV	
13. The pair MP forms a rectangle, replace it with IF	

Hasil Enkripsi

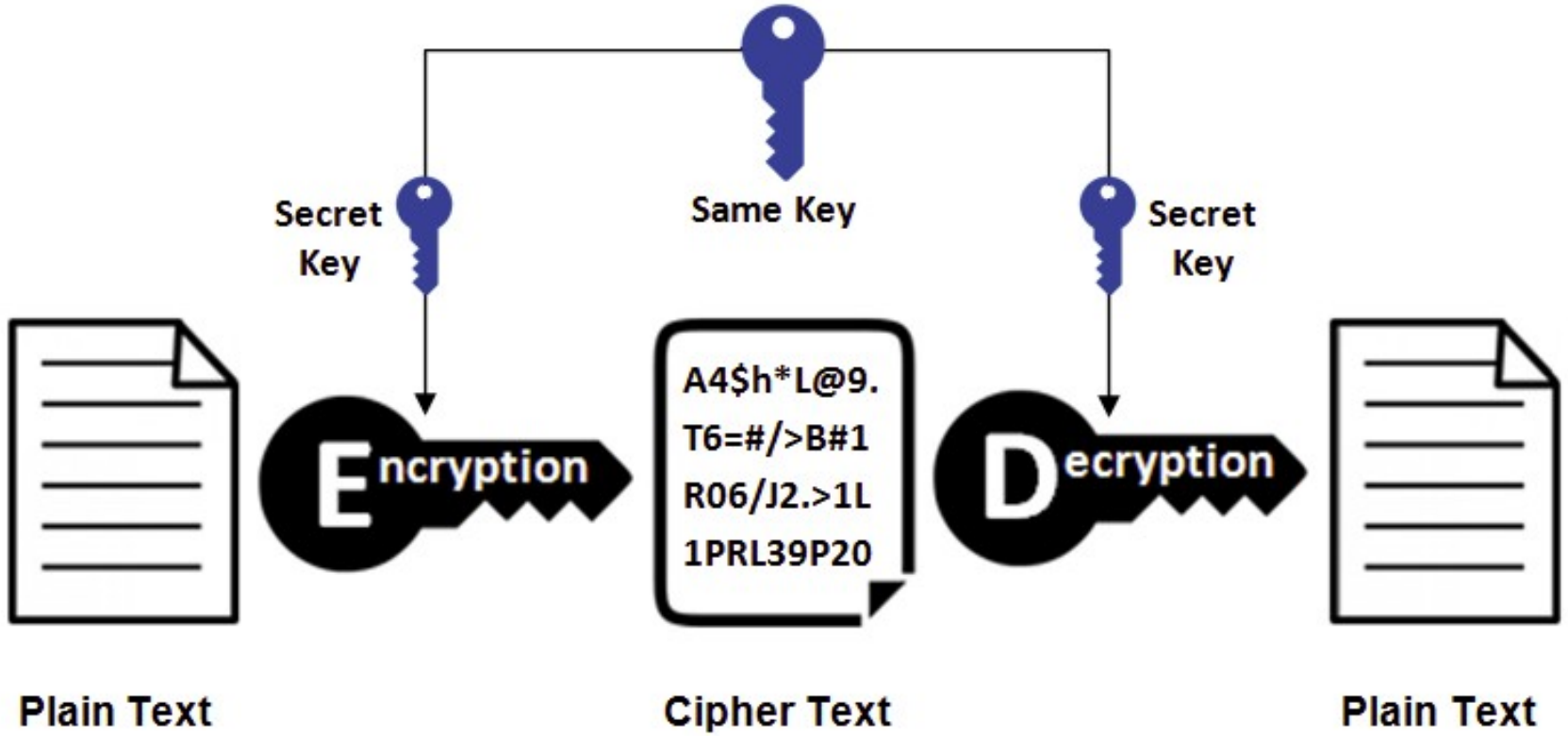
3. Hasil enkripsi menjadi:

   BMODZ BXDNA BEKUD MUIXM MOUVI F

Single key cryptography

- *Single key cryptography* dikenal dengan istilah *symmetric key cryptography*.
- Pada jenis *cryptography* ini, enkripsi dan dekripsi data terjadi dengan menggunakan sebuah *secret key*.
- Pengirim dan juga penerima harus memiliki *secret key*.
- Beberapa algoritma *secret key* telah dikembangkan, diantaranya:
  - Data Encryption Standard (DES)
  - Triple Data Encryption Standard (3DES)
  - International Data Encryption Algorithm (IDEA)

Ilustrasi Symmetric Encryption



Contoh Enkripsi Symmetric Key

- Untuk menerapkan enkripsi data *symmetric key*, Anda dapat menggunakan tool openssl. Contoh:

```
$ openssl enc -des3 -in data.txt -out data.txt.enc
```

- Perintah di atas mengenkripsi file data.txt dengan algoritma enkripsi DES3
- Saat Anda eksekusi perintah di atas, maka Anda akan ditanyakan *password*.

Contoh Enkripsi Symmetric Key

- Untuk mendekripsi data menggunakan *symmetric key*, Anda dapat menggunakan tool openssl. Contoh:

```
$ openssl enc -d -des3 -in data.txt.enc -out data.txt
```

- Perintah di atas mendekripsi file data.txt.enc dengan algoritma DES3.
- Saat Anda eksekusi perintah di atas, maka Anda akan ditanyakan *password*.

Public key cryptography

- *Public key cryptography* menggunakan sepasang kunci (*pair of keys*) bukan sebuah kunci (sebagaimana dalam Secret key cryptography) untuk melakukan proses enkripsi dan dekripsi.
- Dalam proses ini, sebuah *key* digunakan untuk enkripsi dan *key* yang lainnya digunakan untuk dekripsi.
- Proses ini dikenal dengan istilah *asymmetric cryptography* karena kedua *key* tersebut diperlukan untuk melaksanakan proses enkripsi dan dekripsi, dan kedua *key* berdasarkan algoritma yang berbeda.

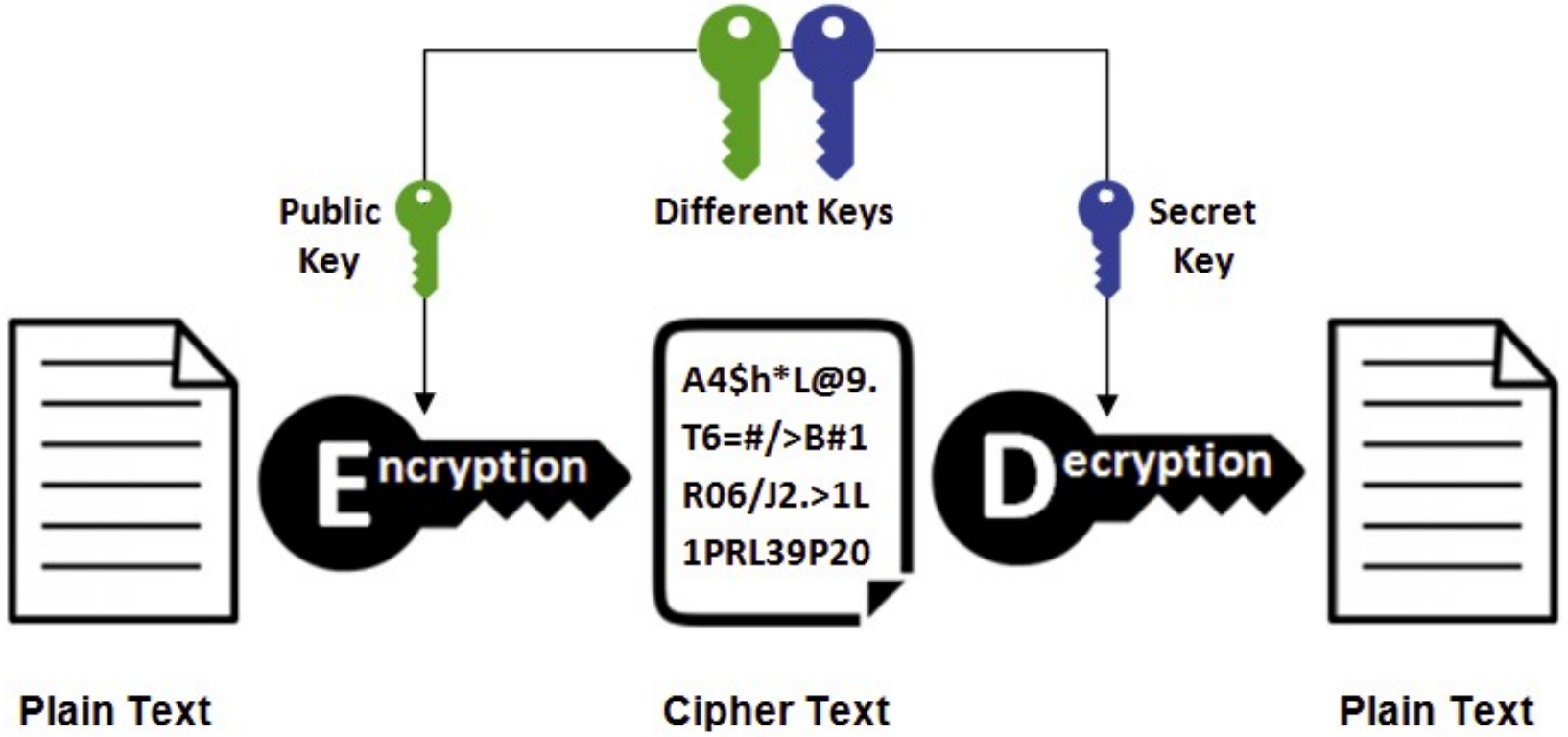
Public key cryptography

- Dalam *public key cryptography*, satu *key* didistribusikan secara bebas ke pengguna lainnya.
- *Key* ini disebut *public key* dan digunakan untuk enkripsi.
- Dan kunci yang satunya lagi disebut *private key*, digunakan untuk proses dekripsi dan hanya disimpan / dipegang oleh si pemilik (tidak didistribusikan ke pengguna lain).

Public key cryptography

- Data yang dienkripsi dengan *public key* dapat didekripsi hanya dengan *private key* yang bersangkutan.
- Dan sebaliknya, data yang dienkripsi dengan *private key* hanya dapat didekripsi oleh *public key* yang bersangkutan.
- Algoritma yang populer dari *asymmetric encryption* adalah RSA encryption.

Ilustrasi Asymmetric Encryption



Pesantren Teknologi Informasi dan Komunikasi

PeTIK

Creates Future Skilled Professionals

Jalan Mandor Basar Nomor 54, RT. 01/001, Rangkapanjaya,
Pancoran Mas, Kota Depok 16435

www.petik.or.id

021 7788 6691

info@petik.or.id