
CRYPTOGRAPHY


IN OUR CLASSROOM
WE RESPECT EACH OTHER.
WE TRY OUR BEST.
WE ARE A TEAM.
WE LEARN FROM MISTAKES.
WE CREATE.
WE CELEBRATE EACH OTHER'S SUCCESS.
TEACHFACTORY.COM

CLASSIC/CONVENTIONAL CRYPTOGRAPHY
PART I

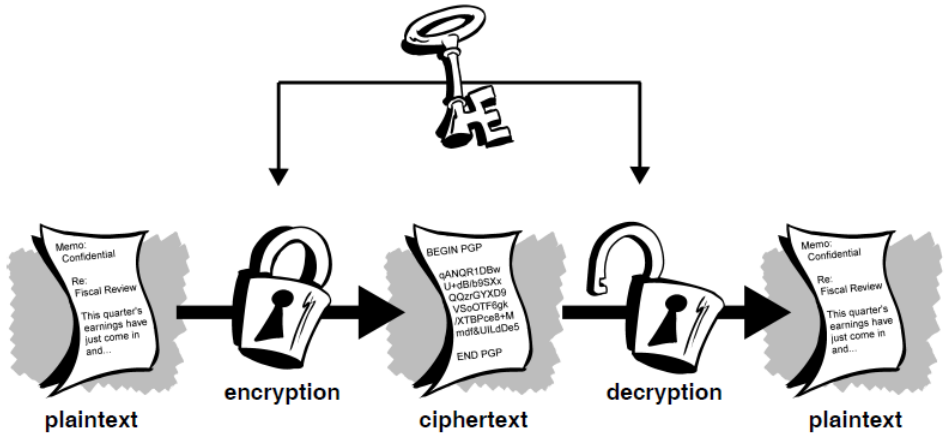
CAPAIAN PEMBELAJARAN

- Mahasiswa memahami klasifikasi dan jenis kriptografi konvensional/klasik
- Mahasiswa memahami cara kerja beberapa jenis kriptografi konvensional/klasik

Agenda.

- Conventional cryptography and clasification

CONVENTIONAL CRYPTOGRAPHY



5

CONVENTIONAL CRYPTOGRAPHY

- Kriptogrfi konvensional terbagi ke dalam 9 klasifikasi
  - Monoalphabetic - Caesar's chiper, ROT13, Four Square chiper
  - Polyalphabetic - Running Key, Vigenere, One Time Pad
  - Polygraphic - Playfair, Trifid
  - Route Transposition - Rail Fence
  - Synchronous Stream - A5/1
  - Asynchronous Stream - Rabbit, Autokey
  - Iterated Block - AES, Blowfish, DES, IDEA, SMS4
  - Fractionated Block - ADFGVX, Stradding Checkboard
  - Steganigraphic - Bacon

6

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Caesar's Chiper

- **Caesar's chiper** adalah contoh kriptogrfi konvensional **monoalphabetic** yang digunakan oleh Julius Caesar untuk mengirimkan pesan kepada bawahannya dan sekutunya.
- Caesar's chiper dilakukan dengan cara melakukan enkripsi pada setiap huruf alfabet dengan melakukan penggeseran (shifting) urutan alfabet.
- Contoh:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get

DEFGHIJKLMNOPQRSTUVWXYZABC

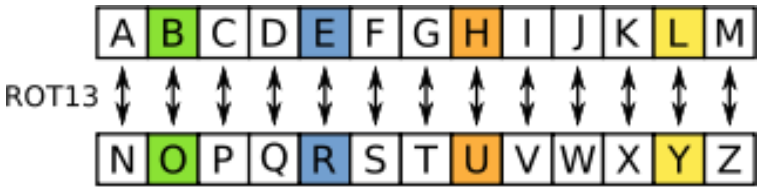
where D=A, E=B, F=C, and so on.

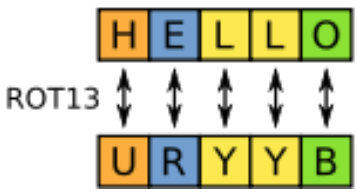
7

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

ROT13 Chiper

- Contoh lainnya dalam penggunaan kriptogrfi konvensional adalah **ROT13** dan **Four Square Chiper**
- **ROT13** menggantikan setiap huruf dengan mitranya 13 karakter lebih jauh di sepanjang alfabet.



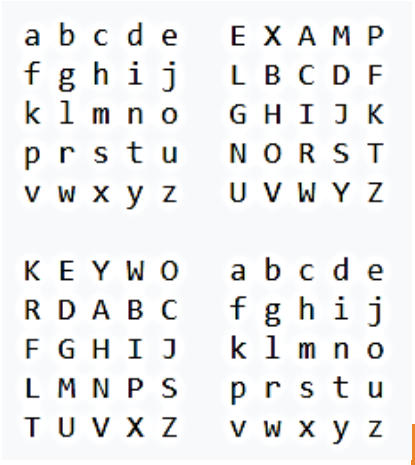


8

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Four Square Chiper

- **Four Square Chiper** menggunakan urutan alfabet yang disajikan dalam bentuk kubus (*square*) berjumlah 4 buah
- Setiap alfabet dalam *plaintext* kemudian digantikan oleh setiap alfabet pada kubus alfabet lainnya.
- Pengaturan huruf dalam kubus dapat diatur sedemikian rupa sesuai kesepakatan antara enkriptor dan dekriptor.



9

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Vigenere Chiper

- Kode *vigènere* termasuk kode abjad-majemuk (*polyalphabetic substitution cipher*).
- Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16, tahun 1586.
- Algoritma ini baru dikenal luas 200 tahun kemudian dan dinamakan kode *vigènere*.
- *Vigènere* merupakan pemicu perang sipil di Amerika dan kode *vigènere* digunakan oleh Tentara Konfederasi (*Confederate Army*) pada perang sipil Amerika (*American Civil War*).
- Kode *vigènere* berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19. (Ariyus, 2008).

10

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Vigenere Chiper

- Teknik untuk menghasilkan *ciphertext* bisa dilakukan menggunakan substitusi angka maupun bujursangkar *vigènere*. Teknik susbtitusi *vigènere* dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser.

Contoh:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
DAN SETERUSNYA...																									

11

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Vigenere Chiper

Contoh kasus: Menentukan cipherteks dari plainteks "Dzulfikar" dengan key "Kevin"

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

D	Z	U	L	F	I	Q	A	R
3	25	20	11	5	8	16	0	17

K	E	V	I	N
10	4	21	8	13

12

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Vigenere Chiper

Penyelesaian:

D	Z	U	L	F	I	Q	A	R
3	25	20	11	5	8	16	0	17
+								
K	E	V	I	N	K	E	V	I
10	4	21	8	13	10	4	21	8
=								
13	29	41	19	18	18	20	21	25

13

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Vigenere Chiper

Penyelesaian:

D	Z	U	L	F	I	Q	A	R
3	25	20	11	5	8	16	0	17
+								
K	E	V	I	N	K	E	V	I
10	4	21	8	13	10	4	21	8
=								
13	29	41	19	18	18	20	21	25

14

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Vigenere Chiper

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
DAN SETERUSNYA																									

N	D	P	T	S	S	U	V	Z
13	29	41	19	18	18	20	21	25

15

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Running Key Chiper

- Running Key Cipher merupakan cara enkripsi yang mirip seperti Vigenere. Perbedaannya terletak pada kunci yang dipilih.
- Running Key memiliki sandi kunci yang mirip seperti kutipan dari sebuah buku.
- Kunci untuk menjalankan Running Key adalah dengan memasukan sebuah kalimat utama yang kemudian di enkripsi menggunakan sebuah kalimat kunci untuk kemudian di sandikan dengan tabel (Tabula Recta) dan dapatlah Cipher Text

16

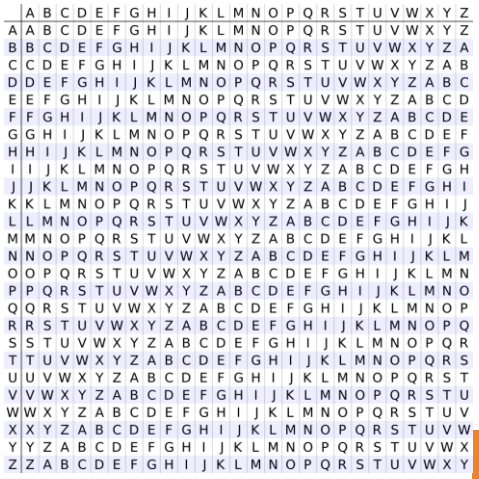
CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

Running Key Chiper

Tabula Recta.

- Tabula Recta adalah tabel persegi huruf, yang setiap barisnya dibuat dengan menggeser yang sebelumnya ke kiri.
- Istilah ini ditemukan oleh penulis dan biarawan Jerman Johannes Trithemius pada tahun 1508, dan digunakan dalam sandi Trithemius-nya.

(Sumber:Wikipedia)



17

CONVENTIONAL CRYPTOGRAPHY AND CLASIFICATION

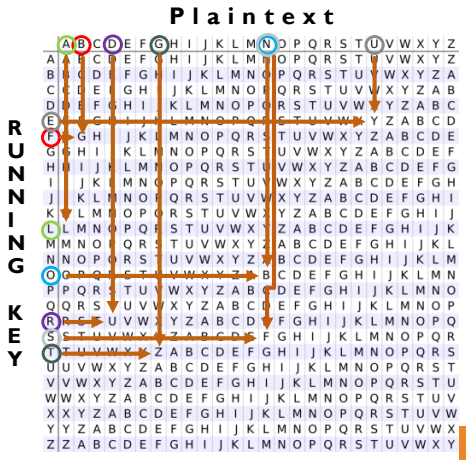
Running Key Chiper

Enkripsi.

Plaint text	B	A	N	D	U	N	G
Running key	f	l	o	r	e	s	t
Cipher text	**G**	**L**	**B**	**U**	**Y**	**F**	**Z**

Prosedur.

1. Pilih karakter plain text pada baris paling atas
2. Pilih karakter running key pada kolom paling kiri
3. Tarik garis lurus membentuk siku antara karakter *plaintext* dengan *running key* maka didapatkan hasil *ciphertext*



18

CLASSIC/CONVENTIONAL CRYPTOGRAPHY PART I