

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.


MODERN CRYPTOGRAPHY PART I



CAPAIAN PEMBELAJARAN

- Mahasiswa memahami konsep kriptografi modern
- Mahasiswa memahami kategori chipper

Agenda.

- Kriptografi modern
- Kategori **chipper**
 - **Stream cipher**
 - **Block cipher**

KRIPTOGRAFI MODERN

- Kriptografi terbagi dalam 2 kelompok besar: (1) kriptografi sebelum era komputer digital; dan (2) kriptografi pada era digital.
- Kriptografi sebelum era komputer digital: **kriptografi klasik/konvensional** (huruf).
- Kriptografi pada era digital: **kriptografi modern** (biner).
- Kriptografi modern masih menggunakan dua teknik dasar kriptografi klasik, yaitu **permutasi** dan **transposisi**.
- Kriptografi modern menggunakan algoritma yang kompleks untuk mempersulit kriptanalisis untuk memecahkan ciperteks.

5

KRIPTOGRAFI MODERN

Rangkaian Bit dan Operasi.

- Plainteks, kunci, dan ciperteks direpresentasikan dalam biner.
- Beberapa algoritma kriptografi modern memproses data dalam bentuk blok-blok bit.
- Rangkaian bit dipecah menjadi blok-blok bit dan dituliskan dalam sejumlah cara bergantung pada panjang blok.
- Contoh: Bit 100110100111
- Jika panjang bit tidak habis dibagi dengan ukuran blok yang ditetapkan, maka blok yang terakhir ditambahkan bit-bit semu, **padding bit**.

6

KRIPTOGRAFI MODERN

- Cara lain adalah dengan merepresentasikan setiap blok-blok bit ke dalam bilangan HEX dan dengan melakukan operasi XOR sederhana, yaitu:
 - Enkripsi : $C = P \oplus K$
 - Dekripsi : $P = C \oplus K$
- **Contoh:** menentukan cipherteks dari plainteks **110110001101001111** menggunakan representasi:
 1. HEX; dan
 2. XOR dengan key = 5.

ASCII control characters		ASCII printable characters				Extended ASCII characters									
00	NULL (Null character)	32	space	64	@	96	`	128	Ç	160	à	192	Ł	224	Ó
01	SOH (Start of Header)	33	!	65	A	97	a	129	ü	161	í	193	ł	225	ô
02	STX (Start of Text)	34	"	66	B	98	b	130	é	162	ó	194	Ł	226	ö
03	ETX (End of Text)	35	#	67	C	99	c	131	â	163	ú	195	ł	227	õ
04	EOT (End of Trans.)	36	\$	68	D	100	d	132	ä	164	ñ	196	—	228	ö
05	ENQ (Enquiry)	37	%	69	E	101	e	133	à	165	Ñ	197	ł	229	ó
06	ACK (Acknowledgement)	38	&	70	F	102	f	134	á	166	ª	198	ä	230	µ
07	BEL (Bell)	39	'	71	G	103	g	135	ç	167	º	199	Á	231	þ
08	BS (Backspace)	40	(72	H	104	h	136	ê	168	¿	200	Ĺ	232	þ
09	HT (Horizontal Tab)	41)	73	I	105	i	137	ë	169	®	201	ł	233	Ů
10	LF (Line feed)	42	*	74	J	106	j	138	è	170	™	202	ł	234	Ů
11	VT (Vertical Tab)	43	+	75	K	107	k	139	ï	171	½	203	ł	235	Ů
12	FF (Form feed)	44	,	76	L	108	l	140	î	172	¼	204	ł	236	ÿ
13	CR (Carriage return)	45	-	77	M	109	m	141	í	173	⅓	205	ł	237	ÿ
14	SO (Shift Out)	46	.	78	N	110	n	142	Ā	174	«	206	ł	238	—
15	SI (Shift In)	47	/	79	O	111	o	143	Ā	175	»	207	ł	239	.
16	DLE (Data link escape)	48	0	80	P	112	p	144	Ē	176	⋯	208	ó	240	≡
17	DC1 (Device control 1)	49	1	81	Q	113	q	145	æ	177	⋮	209	Đ	241	±
18	DC2 (Device control 2)	50	2	82	R	114	r	146	Æ	178	⋮	210	Ě	242	¼
19	DC3 (Device control 3)	51	3	83	S	115	s	147	ó	179	⋮	211	Ě	243	½
20	DC4 (Device control 4)	52	4	84	T	116	t	148	ô	180	⋮	212	Ě	244	¾
21	NAK (Negative acknowl.)	53	5	85	U	117	u	149	õ	181	Ā	213	ı	245	\$
22	SYN (Synchronous idle)	54	6	86	V	118	v	150	û	182	Ā	214	ı	246	+
23	ETB (End of trans. block)	55	7	87	W	119	w	151	ü	183	Ā	215	ı	247	,
24	CAN (Cancel)	56	8	88	X	120	x	152	ÿ	184	©	216	ı	248	.
25	EM (End of medium)	57	9	89	Y	121	y	153	Ŏ	185	ł	217	ł	249	..
26	SUB (Substitute)	58	:	90	Z	122	z	154	Ů	186	ł	218	ł	250	...
27	ESC (Escape)	59	;	91	[123	{	155	ø	187	ł	219	ł	251	!
28	FS (File separator)	60	<	92	\	124		156	£	188	ł	220	ł	252	²
29	GS (Group separator)	61	=	93]	125	}	157	ø	189	ø	221	ł	253	³
30	RS (Record separator)	62	>	94	^	126	~	158	x	190	Ÿ	222	ı	254	⁴
31	US (Unit separator)	63	?	95	_			159	f	191	ł	223	ł	255	nbsp
127	DEL (Delete)														

Sumber: <https://theascii.com.ar/>

KRIPTOGRAFI MODERN

Kasus Latihan #1.

Tentukan plainteks dari chiperteks berikut menggunakan metode dekripsi representasi: HEX

5 3 4 9 4 1 5 0 2 0 4 E 4 4 4 1 4 E 2 1

9

KRIPTOGRAFI MODERN

Kasus Latihan #2.

Tentukan plainteks dari chiperteks berikut menggunakan metode dekripsi XOR dengan $key=5$.

1 8 1 4 1 E 1 2 1 B

10

KATEGORI CIPHER

- Cipher terbagi atas 2 kategori:

- **Stream Cipher**

Algoritma kriptografi yang memproses plainteks/cipherteks dalam bentuk bit tunggal (byte tunggal), dimana cipher mendekripsi satu bit atau satu byte setiap saat.

- **Block Cipher**

Algoritma kriptografi yang memproses plainteks/cipherteks dalam bentuk blok-blok bit (blok byte). Rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan. Misal: pesan dalam 64 bit, maka cipher memproses setara 8 karakter.

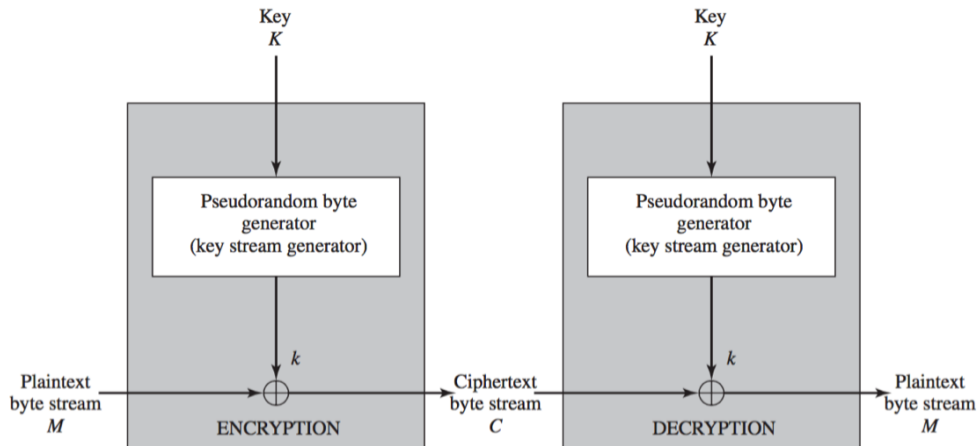
11

STREAM CIPHER

- **Stream cipher** pertama kali dikenalkan oleh Vernam (algoritma vernam).
- Disebut juga sebagai cipher status, karena enkripsi tiap bit bergantung kepada status saat ini (*current status*).
- Proses enkripsi dilakukan dengan melakukan operasi XOR setiap bit plainteks dengan key yang sudah ditentukan, begitu juga sebaliknya untuk mendekripsikan chiperteks.
- Key pada **stream cipher** dikenal dengan nama **keystream** (aliran kunci) yang dibangkitkan oleh sebuah pembangkit **keystream (keystream generator)**.

12

STREAM CIPHER



Sumber: https://3.bp.blogspot.com/-j9D_lwXAJ7Q/WSwG-tGEjI/AAAAAAAAARI/Is0nmnChwollbQjBT7UAZ0HvzAxjxcwgCLcB/s1600/Untitled.png

13

STREAM CIPHER

- Tingkat keamanan kriptografi stream cipher bergantung pada **keystream generator**.
 - Bit keystream = 0
 - Bit keystream dengan pola bit yang berulang
 - Bit keystream acak (**truly random**)

14

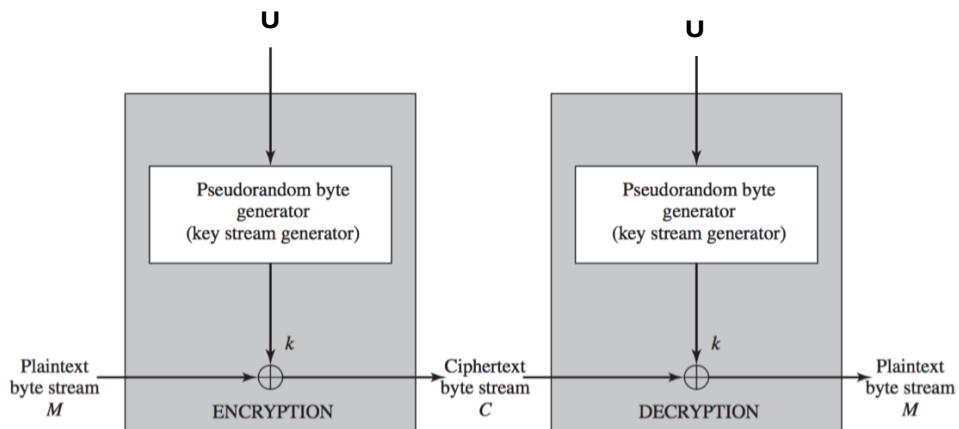
STREAM CIPHER | KEYSTREAM GENERATOR

Keystream Generator.

- Pembangkit kunci-alir diimplementasikan sebagai prosedur algoritmik dimana bit-bit kunci-alir akan dibangkitkan secara simultan.
- Prosedur algoritmik menerima masukan sebuah umpan (*seed*) U sebagai external key yang diberikan oleh pihak pengirim atau penerima pesan.
- Luaran prosedur tersebut merupakan sebuah fungsi U .
- Penerima dan pengirim harus menghasilkan bit-bit kunci yang sama dengan syarat keduanya memiliki umpan U yang sama.

15

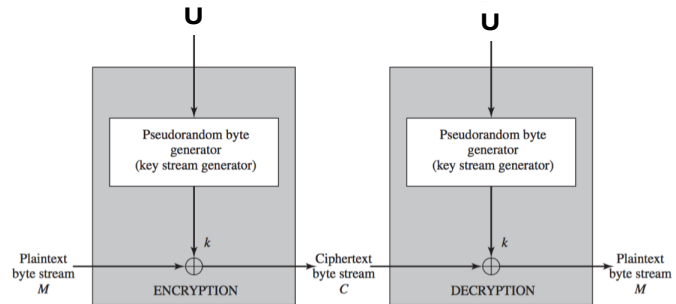
STREAM CIPHER | KEYSTREAM GENERATOR



16

STREAM CIPHER | KEYSTREAM GENERATOR

- Cipher alir menggunakan kunci U yang pendek untuk membangkitkan bit-bit kunci yang panjang
- Persamaan yang digunakan adalah $2^n - 1$, dimana n adalah banyaknya U bit.
- Bit-bit kunci –alir akan berulang hingga mencapai nilai persamaan tersebut.



17

STREAM CIPHER

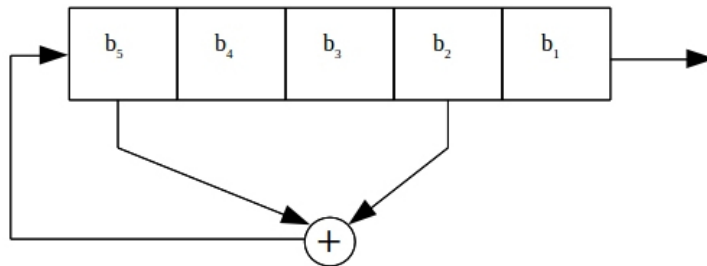
Linier Feedback Shift Register (LFSR).

- Menggunakan register umpan-balik untuk membangkitkan kunci-alir.
- Register geser (*shift*) merupakan perangkat keras berupa sel-sel memori yang dapat digeser ke kiri maupun ke kanan sejauh satu sel.
- Terdiri dari 2 bagian:
 1. Register geser, yaitu barisan bit-bit $(b_n b_{n-1} \dots b_4 b_3 b_2 b_1)$ yang panjangnya n (register geser n bit)
 2. Fungsi umpan-balik, yaitu fungsi yang menerima masukan dari register geser dan mengembalikan nilai fungsi ke register geser.

18

STREAM CIPHER | LFSR

- Fungsi umpan balik adalah operasi XOR bit-bit tertentu di dalam register
- Perhatikan contoh LFSR 4-bit berikut.



Sumber: <https://i.stack.imgur.com/1RUR9.jpg>

19

STREAM CIPHER | LFSR

- Contoh kasus: Tentukan barisan bit-bit luaran dari *stream cipher* jika diketahui register diinisialisasi dengan bit 1 1 1 1.

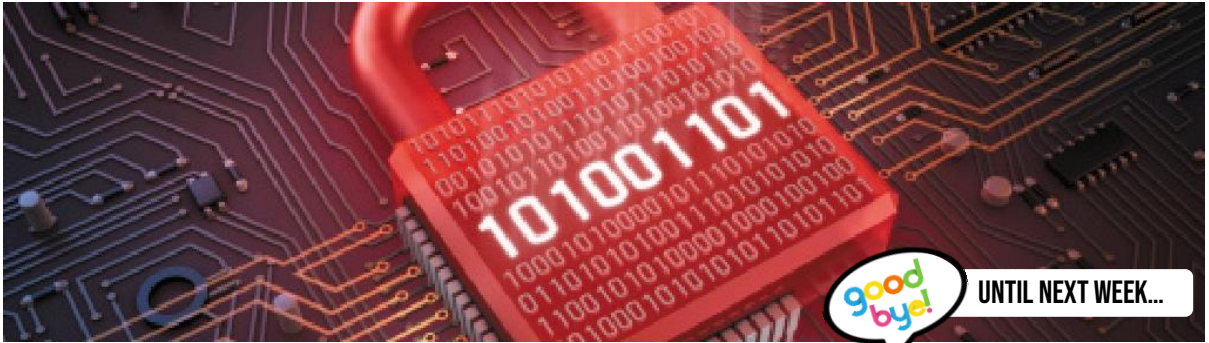
Jawab.

i	Isi Register	Luaran
0	1 1 1 1	
1	0 1 1 1	1
2	1 0 1 1	1
3	0 1 0 1	1
4	1 0 1 0	1
5	1 1 0 1	0
...

Bit luaran akan terus muncul dan berulang hingga fungsi $2^n - 1$ tercapai.

20

MODERN CRYPTOGRAPHY PART I



UNTIL NEXT WEEK...