
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

MODERN CRYPTOGRAPHY
PART 2

CAPAIAN PEMBELAJARAN

- Mahasiswa memahami konsep kriptografi modern
- Mahasiswa memahami kategori chipper

Agenda.

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

4

STREAM CIPHER | ATTACK

Known-Plainteks Attack.

- Misalkan kriptanalisis memiliki potongan plainteks (P) dan cipherteks (C) yang berkoresponden.
- Contoh kasus: Misalkan potongan plainteks `01100101` dienkripsi dengan potongan cipherteks `00110101` ?

  Jawab.

  Dengan menggunakan fungsi deksripsi $\boldsymbol{P} = \boldsymbol{C} \quad \boldsymbol{K}$, maka kriptanalisis dapat menemukan key ($\boldsymbol{K}$) yang berkoresponden.

5

STREAM CIPHER | ATTACK

Cipherteks-Only Attack.

- Serangan yang terjadi terhadap potongan $plainteks$ yang berbeda yang digunakan sebanyak 2 kali.
- Serangan ini disebut dengan $keystream\ reuse\ attack$.
- Contoh kasus: Misalkan kriptanalisi memiliki dua potongan $cipherteks$ berbeda (C1 dan C2) yang dienkripsi menggunakan bit-bit kunci yang sama.

  Kriptanalisis kemudian melakukan operasi XOR terhadap kedua $cipherteks$ tersebut untuk mendapatkan dua buah $plainteks$ yang berbeda.

6

STREAM CIPHER | ATTACK

Flip-bit Attack.

- Serangan ini cenderung untuk mengubah bit $cipherteks$ daripada menemukan kunci atau mengungkap $plainteks$ dari $cipherteks$ yang berkorespondensi.
- Serangan ini biasanya dilakukan oleh $man - in - the - middle$ untuk mengubah pesan yang dikirimkan melalui jalur komunikasi.
- Perubahan yang dilakukan dengan cara membalikkan (flip) bit tertentu, `0` menjadi `1` atau `1` menjadi `0`.

7

BLOCK CIPHER | MODE OPERASI

- Mode operasi dalam kategori cipher blok terbagi menjadi 5 mode
  - $Electronic\ Code\ Book\ (ECB)$
  - $Cipher\ Blok\ Caining\ (CBC)$
  - $Cipher\ Feedback\ (CFB)$
  - $Output\ Feedback\ (OFB)$
  - $Counter\ Mode\ (CoM)$
- Setiap mode memiliki mekanisme dasar yang sama hanya berbeda dalam prosedur enkripsi dan dekripsinya.
- Mode operasi cipher blok pada dasarnya membagi rangkaian bit-bit plainteks dibagi menjadi blok-blok bit berukuran sama panjang.

8

BLOCK CIPHER | MODE OPERASI

- Setiap blok bit plainteks dienkripsi dengan bit-bit kunci yang panjangnya sama dengan blok plainteks.
- Enkripsi menghasilkan blok cipherteks yang berukuran sama dengan blok plainteks.
- Blok cipherteks dienkripsi dengan kunci yang sama.

9

BLOCK CIPHER | MODE OPERASI **ECB**

Electronik Code Book (ECB).

- Setiap blok bit plainteks Pi dienkripsi secara individual dan independen.
- Enkripsi menghasilkan blok cipherteks yang berukuran sama dengan blok plainteks.
- Blok cipherteks dienkripsi dengan kunci yang sama.
- Fungsi enkripsi $C_i = EK(Pi)$
- Fungsi dekripsi $P_i = D_K(Ci)$
- **Contoh kasus.** Menentukan cipherteks dan plainteks **C2AC9** menggunakan kunci (K) D (4 bit)

10

BLOCK CIPHER | MODE OPERASI ECB

Prosedur Enkripsi ECB.

- Membagi plainteks ke dalam blok-blok berukuran 4 bit
- Melakukan operasi XOR setiap blok plainteks dengan bit kunci (K)
- Menggeser ke kiri (*shift left*) setiap bit hasil XOR
- Hasil *shift left* merupakan cipherteks hasil enkripsi
- Mengubah cipherteks ke dalam betuk HEX.

11

BLOCK CIPHER | MODE OPERASI ECB

Prosedur Dekripsi ECB.

- Mengubah cipherteks dalam betuk HEX ke dalam bentuk biner.
- Membagi cipherteks ke dalam blok-blok berukuran 4 bit
- Menggeser ke kanan (*shift right*) setiap bit cipherteks
- Melakukan operasi XOR setiap blok cipherteks dengan bit kunci
- Hasil operasi XOR adalah plainteks.

12

BLOCK CIPHER | MODE OPERASI ECB

Kasus #1.

Lakukanlah enkripsi pesan berikut menggunakan mode operasi ECB dengan kunci C.

KRIPTOGRAFI SERU

13

ASCII control characters

00	NULL	(Null character)
01	SOH	(Start of Header)
02	STX	(Start of Text)
03	ETX	(End of Text)
04	EOT	(End of Trans.)
05	ENQ	(Enquiry)
06	ACK	(Acknowledgement)
07	BEL	(Bell)
08	BS	(Backspace)
09	HT	(Horizontal Tab)
10	LF	(Line feed)
11	VT	(Vertical Tab)
12	FF	(Form feed)
13	CR	(Carriage return)
14	SO	(Shift Out)
15	SI	(Shift In)
16	DLE	(Data link escape)
17	DC1	(Device control 1)
18	DC2	(Device control 2)
19	DC3	(Device control 3)
20	DC4	(Device control 4)
21	NAK	(Negative acknowl.)
22	SYN	(Synchronous idle)
23	ETB	(End of trans. block)
24	CAN	(Cancel)
25	EM	(End of medium)
26	SUB	(Substitute)
27	ESC	(Escape)
28	FS	(File separator)
29	GS	(Group separator)
30	RS	(Record separator)
31	US	(Unit separator)
127	DEL	(Delete)

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Extended ASCII characters

128	Ç	160	á	192	└	224	Ó
129	ü	161	í	193	┴	225	ß
130	é	162	ó	194	┬	226	Ô
131	â	163	ú	195	├	227	Ò
132	ä	164	ñ	196	─	228	õ
133	à	165	Ñ	197	┼	229	Õ
134	å	166	ª	198	ã	230	µ
135	ç	167	º	199	Ã	231	þ
136	ê	168	¿	200	╚	232	Þ
137	ë	169	®	201	╔	233	Ú
138	è	170	¬	202	╩	234	Û
139	ï	171	½	203	╦	235	Ù
140	î	172	¼	204	╠	236	ý
141	ì	173	¡	205	═	237	Ý
142	Ä	174	«	206	╬	238	¯
143	Å	175	»	207	¤	239	´
144	É	176	░	208	ð	240	≡
145	æ	177	▒	209	Ð	241	±
146	Æ	178	▓	210	Ê	242	‗
147	ô	179	│	211	Ë	243	¾
148	ö	180	┤	212	È	244	¶
149	ò	181	Á	213	ı	245	§
150	û	182	Â	214	Í	246	÷
151	ù	183	À	215	Î	247	¸
152	ÿ	184	©	216	Ï	248	°
153	Ö	185	╣	217	┘	249	¨
154	Ü	186	║	218	┌	250	·
155	ø	187	╗	219	█	251	¹
156	£	188	╝	220	▄	252	³
157	Ø	189	¢	221	¦	253	²
158	×	190	¥	222	Ì	254	■
159	ƒ	191	┐	223	▀	255	nbsp

Sumber: https://theasciicode.com.ar/

BLOCK CIPHER | MODE OPERASI CBC

Cipher Block Chaining (CBC).

- Mode CBC digunakan dalam enkripsi transmisi data.
- CBC menerapkan mekanisme *feedback* pada sebuah blok
- Melakukan *feedback* dari proses enkripsi sebelumnya ke proses enkripsi berikutnya
- Melakukan operasi XOR blok plainteks sebelumnya dengan IV (*initialization vector*)
- Hal ini berlangsung hingga blok terakhir plainteks.
- **Contoh kasus.** Tentukan cipherteks dari plainteks **C2AC9** dengan kunci (K) D (4 bit).

15

BLOCK CIPHER | MODE OPERASI CBC

Prosedur Enkripsi CBC.

- Membagi plainteks ke dalam blok-blok berukuran 4 bit
- Melakukan operasi XOR setiap blok plainteks pertama dengan bit C_0 (IV)
- Melakukan operasi XOR hasilnya dengan kunci (K)
- Menggeser ke kiri (*shift left*) setiap bit hasil XOR dengan K
- Hasil ini merupakan C_1
- Mengulang point 2 dengan blok plainteks berikutnya dengan bit cipherteks sebelumnya hingga blok terakhir plainteks

16

BLOCK CIPHER | MODE OPERASI CBC

Kasus #2.

Menetukan prosedur deksripsi untuk meode CBC.

Kasus #3.

Lakukanlah enkripsi pesan berikut menggunakan mode perasi CBC dengan kunci C.

KRIPTOGRAFI SERU

17

BLOCK CIPHER | MODE OPERASI CFB

Cipher-Feedback (CFB).

- Mode ini diterapkan untuk mengatasi permasalahan pada mode CBC.
- Data dienkripsi dalam unit yang lebih kecil daripada ukuran blok.
- Secara umum, CFB p-bit mengenkripsi plainteks sebanyak p bit setiap kalinya.
- CFB melakukan enkripsi chipper blok seperti enkripsi pada *stream cipher*.
- CFB membutuhkan antrian yang berukuran sama dengan ukuranblok masukan.
- CFB menggunakan IV (*initialization vector*) sebagai bit inisiasi proses enkripsi sebagai C_0

18

BLOCK CIPHER | MODE OPERASI CFB

Prosedur Enkripsi FCB.

- Antrian diisi dengan IV (*initialization vector*) seperti pada mode CBC.
- Enkripsi semua string IV di dalam antian dengan kunci K.
- Byte terkiri (*most significant byte*) dari hasil enkripsi berlaku sebagai keystream (k_i)
- Lakukan operasi XOR dengan byte terkiri plainteks untuk mendapatkan cipherteks
- Lakukan *shift left* IV yang terenkripsi dan tambahkan chiperteks ke bagian paling kanan IV terenkripsi sehingga menjadi IV baru
- Ulangi langkah 2 hingga semua planteks terenkripsi.

19

BLOCK CIPHER | MODE OPERASI CFB

- **Contoh kasus.** Menentukan cipherteks dan plainteks X dengan kunci K dan CFB p-bit = 2.

Kasus #4.

Menentukan cipherteks dan plainteks K dengan kunci X dan CFB p-bit = 4.

20

MODERN CRYPTOGRAPHY
PART 2