KRIPTOGRAFI DAN STEGANOGRAFI

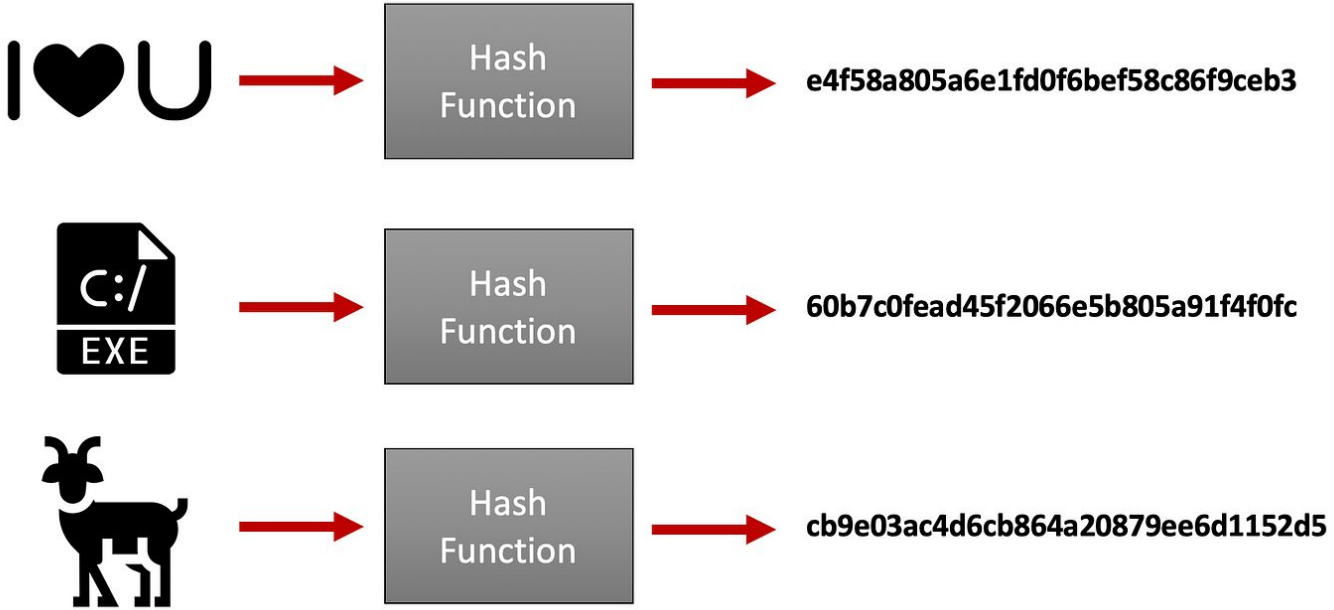
Program Studi Informatika

Sesi 4 – Kriptografi Symmetric

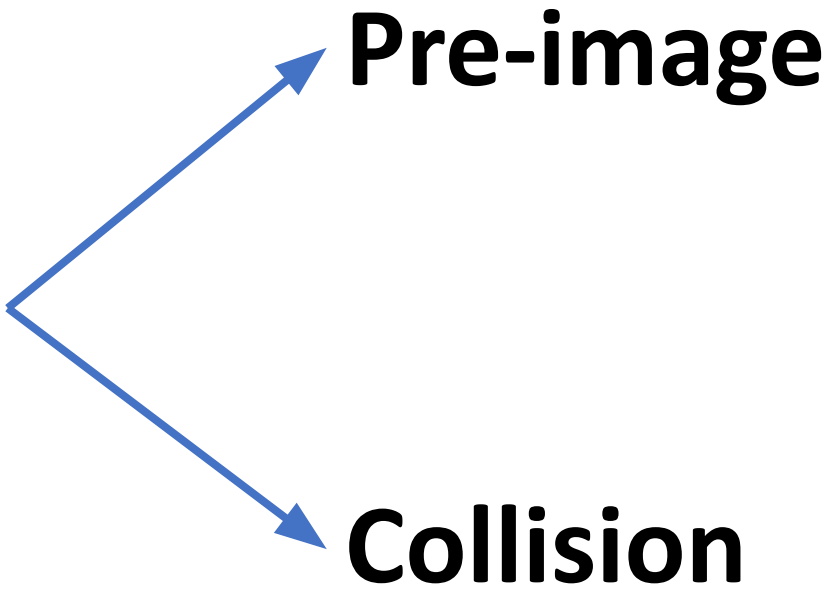
Abdul Azzam Ajhari, S.Kom., M.Kom.

Refreshment Sesi 3

Hash function adalah fungsi matematis yang mengubah data dari ukuran berapa pun menjadi keluaran (output) dengan ukuran tetap yang biasanya berupa string karakter alfanumerik atau angka biner.



Sumber gambar: SecurityBreak


Keamanan
Kriptografi Hash
Pre-image
Collision

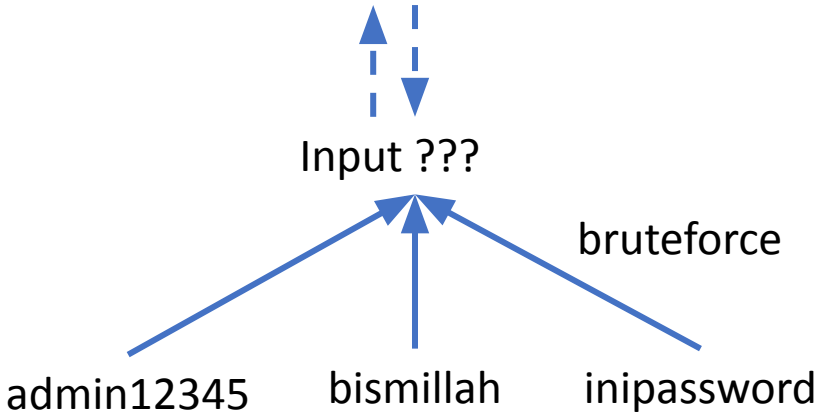
Pre-image resistance (Tahan Pre-image)

Konsep ini mengacu pada kesulitan menemukan input asli jika hanya diberikan nilai hash.

Jika ada sebuah nilai hash $H(x)$ maka sangat sulit untuk menemukan nilai x yang menghasilkan hash tersebut.

Example
Pre-image resistance

Hash:
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd0fa4
d8969d3f80a95



Collision resistance (Tahan Tabrakan)

- Collision resistance berarti sulitnya menemukan dua input berbeda, x dan y dengan $x \neq y$, yang menghasilkan nilai hash yang sama $H(x) = H(y)$.

Example
Collision resistance

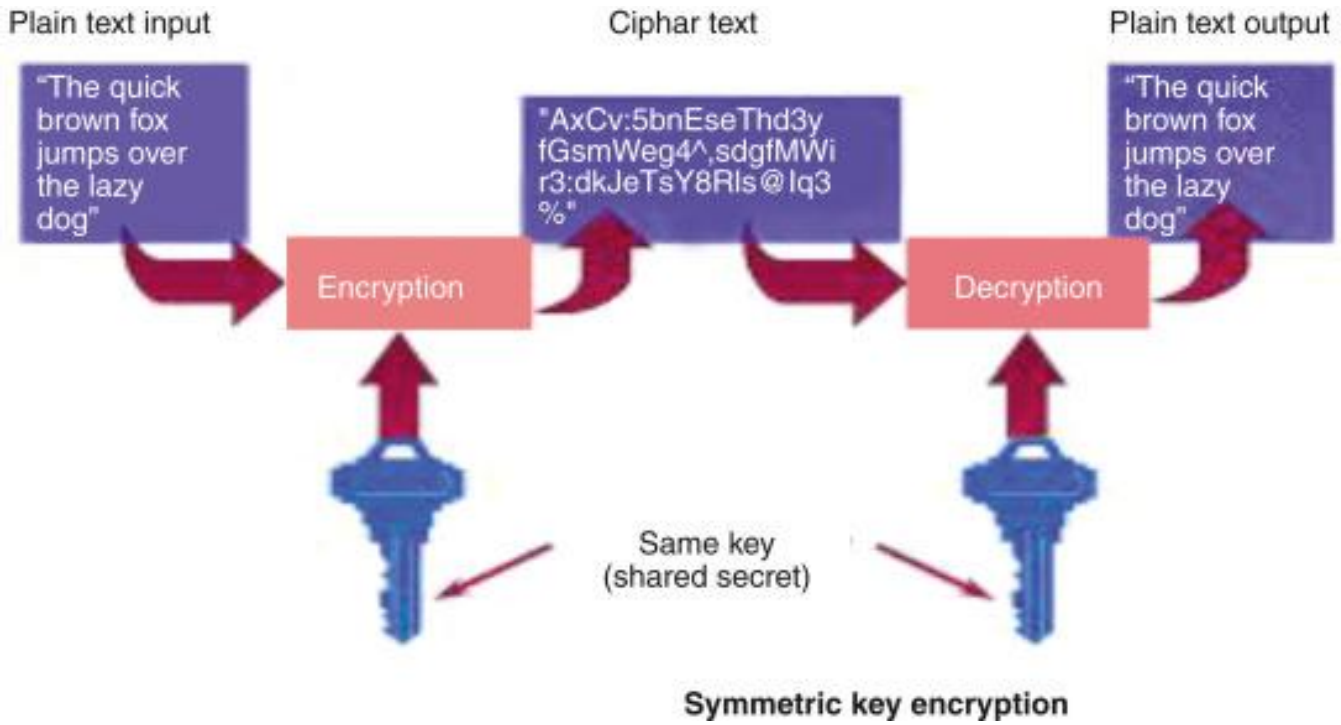
HASH $H(x) = H(y)$:
59266e8b0ae7f28babf85df
d54653f33695d04bcfc944
48985c5e3fa15a85ba6

HASH x:
51ac881397b1afb277a1ba
19e97f688efd6cab5ae4f2f
175c6f9e0e34fd74d31

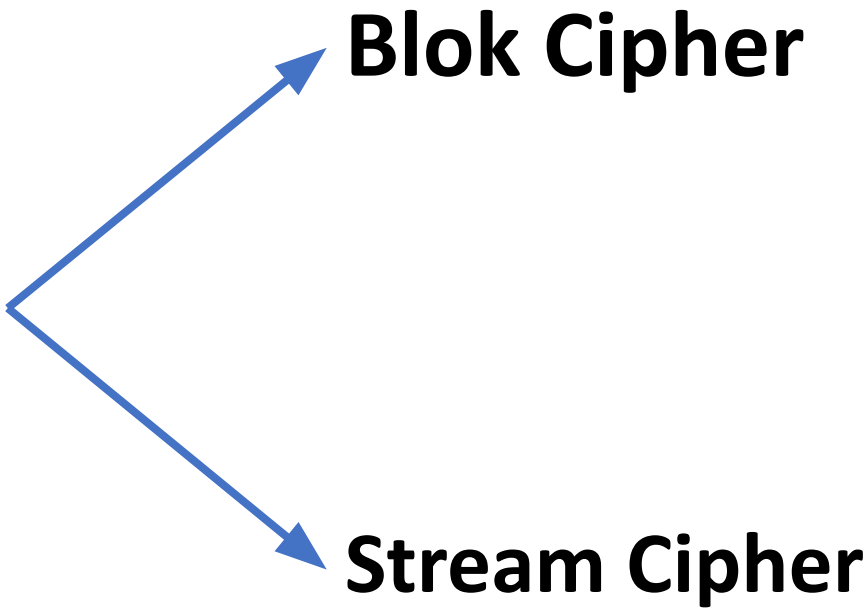
HASH y:
06a1ed7fee6aa51f7d2f9b6
6c070fd8a23ef064702c04
d9ed56a18f3468e259c

Kriptografi Symmetric

Kriptografi simetris dikenal sebagai kriptografi kunci privat, kunci rahasia, atau enkripsi kunci tunggal. Disebut kriptografi simetris karena menggunakan kunci yang sama untuk enkripsi teks biasa (sending message) dan mendekripsi teks tersandi (receive message).



Symmetric key encryption


Tipe Kriptografi
Symmetric
Blok Cipher
Stream Cipher

Blok Cipher

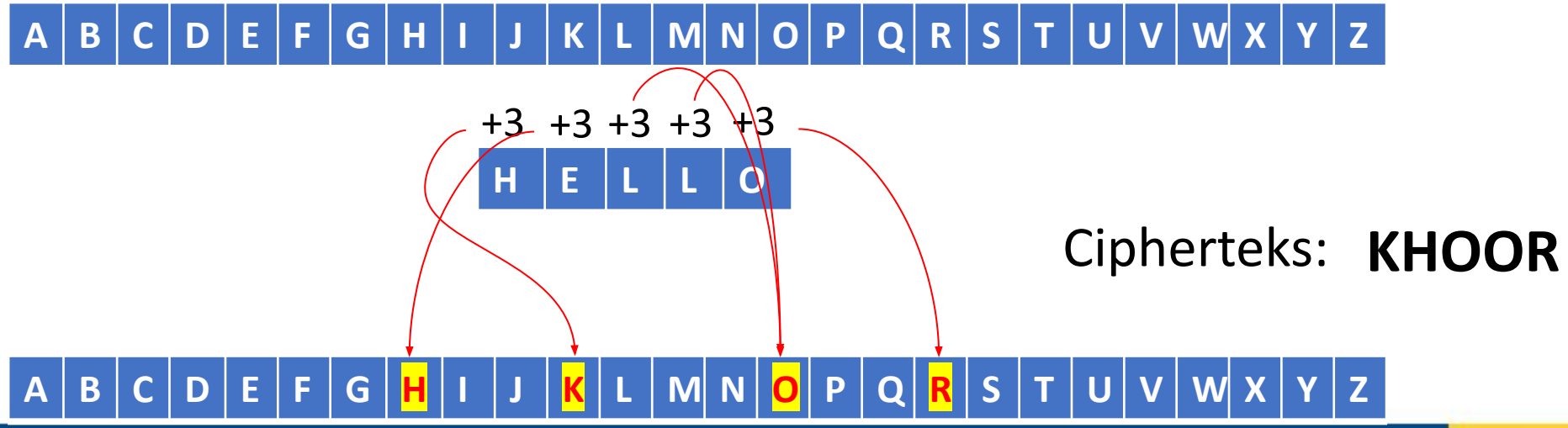
Dalam blok cipher, algoritma Cipher bekerja pada blok data dengan ukuran tetap. Misalnya, jika ukuran blok delapan, delapan byte plaintext dienkripsi sekaligus.

Biasanya, antarmuka pengguna untuk operasi enkripsi/dekripsi menangani data yang lebih panjang dari ukuran blok dengan berulang kali memanggil fungsi sandi tingkat rendah.

Example Blok Cipher dengan Substitusi (Caesar Cipher)

Plainteks: **HELLO** → H E L L O

Key: **3** → Pergeseran sebanyak 3 langkah alfabet

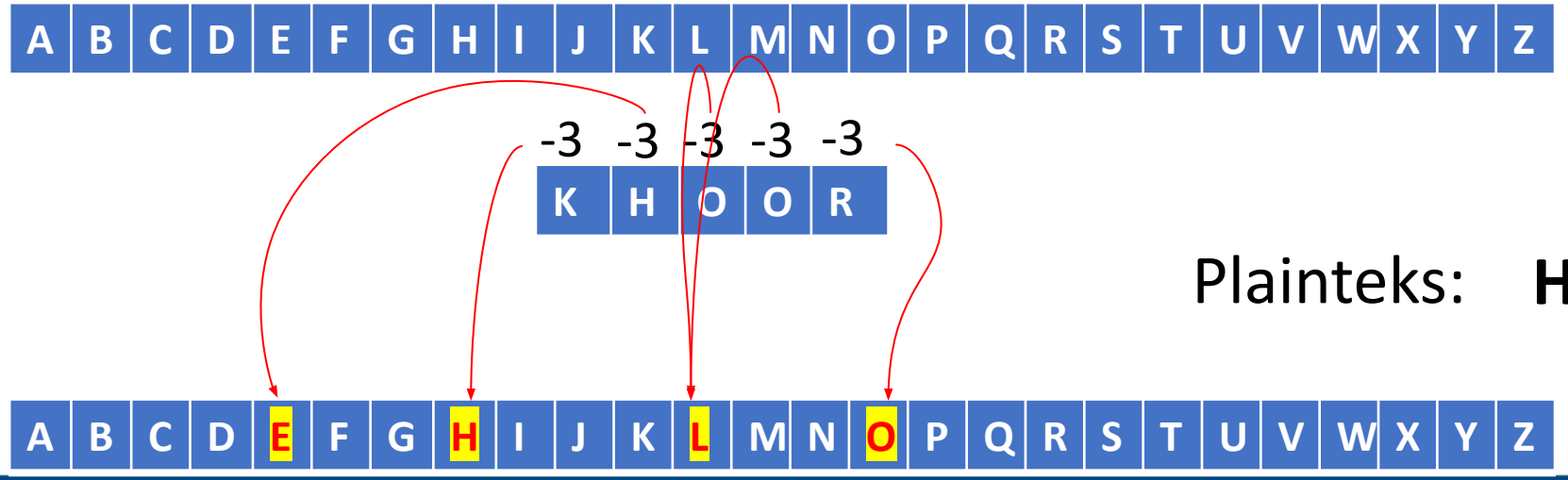


Cipherteks: **KHOOR**

Example Blok Cipher dengan Substitusi (Caesar Cipher)

Cipherteks: **KHOOR** → K H O O R

Key: **3** → Pergeseran sebanyak 3 langkah alfabet (mundur)



Plainteks: **HELLO**

Stream Cipher

Stream cipher tidak bekerja berdasarkan blok, melainkan mengonversi satu bit (atau satu byte) data pada satu waktu.

Pada dasarnya, stream cipher menghasilkan keystream berdasarkan kunci yang disediakan. Keystream yang dihasilkan kemudian di-XOR dengan data plaintext.

Example Stream Cipher dengan XOR

Plainteks: **HELLO**

Key: **XMCKL**

ASCII - Binary Character Table

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

Example Stream Cipher dengan XOR

Plainteks:

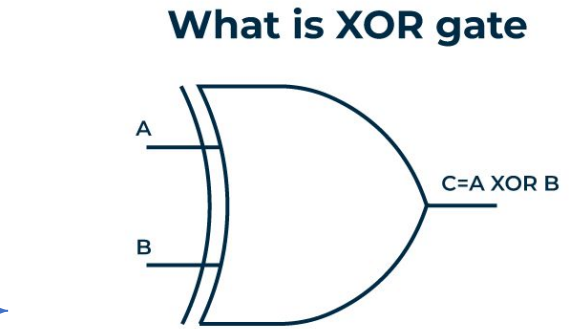
Huruf	ASCII (Decimal)	ASCII (Binary)
H	72	01001000
E	69	01000101
L	76	01001100
L	76	01001100
O	79	01001111

Key:

Huruf	ASCII (Decimal)	ASCII (Binary)
X	88	01011000
M	77	01001101
C	67	01000011
K	75	01001011
L	76	01001100

Example Stream Cipher dengan XOR

Plainteks:		Key:		Biner:
H (01001000)		X (01011000)		00010000
E (01000101)		M (01001101)		00001000
L (01001100)	XOR	C (01000011)	=	00001111
L (01001100)		K (01001011)		00000111
O (01001111)		L (01001100)		00000011



Truth Table of XOR gate

A	B	C=A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

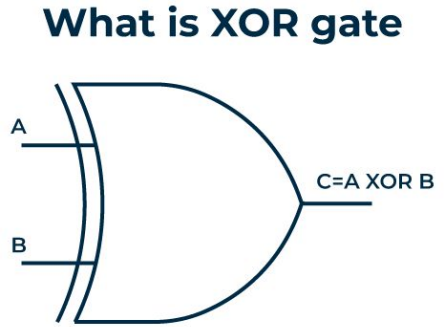
Example Stream Cipher dengan XOR

Biner:	ASCII Decimal	Cipherteks
00010000	16	DLE
00001000	8	BS
00001111	15	SI
00000111	7	BEL
00000011	3	ETX

ASCII TABLE

Decimal	Hexadecimal	Binary	Octal	Char	Decimal	Hexadecimal	Binary	Octal	Char	Decimal	Hexadecimal	Binary	Octal	Char
0	0	0	0	[NULL]	48	30	110000	60	0	96	60	1100000	140	`
1	1	1	1	[START OF HEADING]	49	31	110001	61	1	97	61	1100001	141	a
2	2	10	2	[START OF TEXT]	50	32	110010	62	2	98	62	1100010	142	b
3	3	11	3	[END OF TEXT]	51	33	110011	63	3	99	63	1100011	143	c
4	4	100	4	[END OF TRANSMISSION]	52	34	110100	64	4	100	64	1100100	144	d
5	5	101	5	[ENQUIRY]	53	35	110101	65	5	101	65	1100101	145	e
6	6	110	6	[ACKNOWLEDGE]	54	36	110110	66	6	102	66	1100110	146	f
7	7	111	7	[BELL]	55	37	110111	67	7	103	67	1100111	147	g
8	8	1000	10	[BACKSPACE]	56	38	111000	70	8	104	68	1101000	150	h
9	9	1001	11	[HORIZONTAL TAB]	57	39	111001	71	9	105	69	1101001	151	i
10	A	1010	12	[LINE FEED]	58	3A	111010	72	:	106	6A	1101010	152	j
11	B	1011	13	[VERTICAL TAB]	59	3B	111011	73	;	107	6B	1101011	153	k
12	C	1100	14	[FORM FEED]	60	3C	111100	74	<	108	6C	1101100	154	l
13	D	1101	15	[CARRIAGE RETURN]	61	3D	111101	75	=	109	6D	1101101	155	m
14	E	1110	16	[SHIFT OUT]	62	3E	111110	76	>	110	6E	1101110	156	n
15	F	1111	17	[SHIFT IN]	63	3F	111111	77	?	111	6F	1101111	157	o
16	10	10000	20	[DATA LINK ESCAPE]	64	40	1000000	100	@	112	70	1110000	160	p
17	11	10001	21	[DEVICE CONTROL 1]	65	41	1000001	101	A	113	71	1110001	161	q
18	12	10010	22	[DEVICE CONTROL 2]	66	42	1000010	102	B	114	72	1110010	162	r
19	13	10011	23	[DEVICE CONTROL 3]	67	43	1000011	103	C	115	73	1110011	163	s
20	14	10100	24	[DEVICE CONTROL 4]	68	44	1000100	104	D	116	74	1110100	164	t
21	15	10101	25	[NEGATIVE ACKNOWLEDGE]	69	45	1000101	105	E	117	75	1110101	165	u
22	16	10110	26	[SYNCHRONOUS IDLE]	70	46	1000110	106	F	118	76	1110110	166	v
23	17	10111	27	[ENG OF TRANS. BLOCK]	71	47	1000111	107	G	119	77	1110111	167	w
24	18	11000	30	[CANCEL]	72	48	1001000	110	H	120	78	1111000	170	x
25	19	11001	31	[END OF MEDIUM]	73	49	1001001	111	I	121	79	1111001	171	y
26	1A	11010	32	[SUBSTITUTE]	74	4A	1001010	112	J	122	7A	1111010	172	z
27	1B	11011	33	[ESCAPE]	75	4B	1001011	113	K	123	7B	1111011	173	{
28	1C	11100	34	[FILE SEPARATOR]	76	4C	1001100	114	L	124	7C	1111100	174	|
29	1D	11101	35	[GROUP SEPARATOR]	77	4D	1001101	115	M	125	7D	1111101	175	}
30	1E	11110	36	[RECORD SEPARATOR]	78	4E	1001110	116	N	126	7E	1111110	176	~
31	1F	11111	37	[UNIT SEPARATOR]	79	4F	1001111	117	O	127	7F	1111111	177	[DEL]
32	20	100000	40	[SPACE]	80	50	1010000	120	P					
33	21	100001	41	!	81	51	1010001	121	Q					
34	22	100010	42	"	82	52	1010010	122	R					
35	23	100011	43	#	83	53	1010011	123	S					
36	24	100100	44	$	84	54	1010100	124	T					
37	25	100101	45	%	85	55	1010101	125	U					
38	26	100110	46	&	86	56	1010110	126	V					
39	27	100111	47	'	87	57	1010111	127	W					
40	28	101000	50	(	88	58	1011000	130	X					
41	29	101001	51	)	89	59	1011001	131	Y					
42	2A	101010	52	*	90	5A	1011010	132	Z					
43	2B	101011	53	+	91	5B	1011011	133	[					
44	2C	101100	54	,	92	5C	1011100	134	\					
45	2D	101101	55	-	93	5D	1011101	135	]					
46	2E	101110	56	.	94	5E	1011110	136	^					
47	2F	101111	57	/	95	5F	1011111	137	_					

Example Stream Cipher dengan XOR

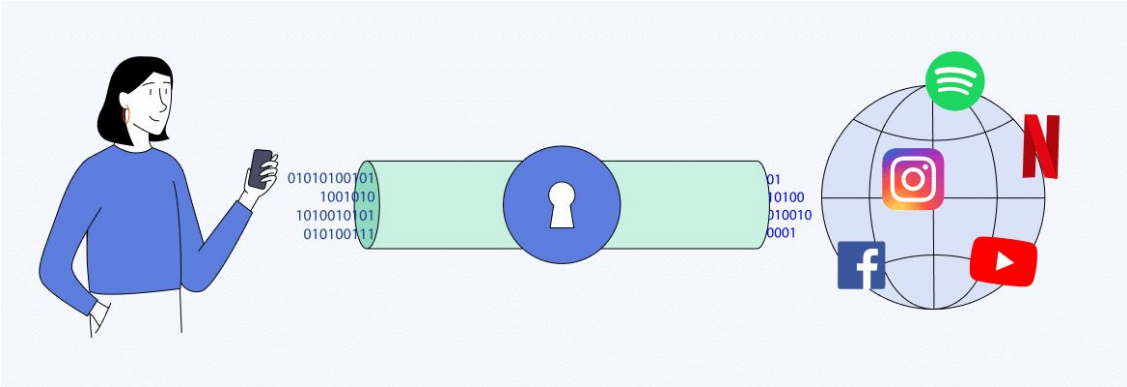


Truth Table of XOR gate

A	B	C=A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

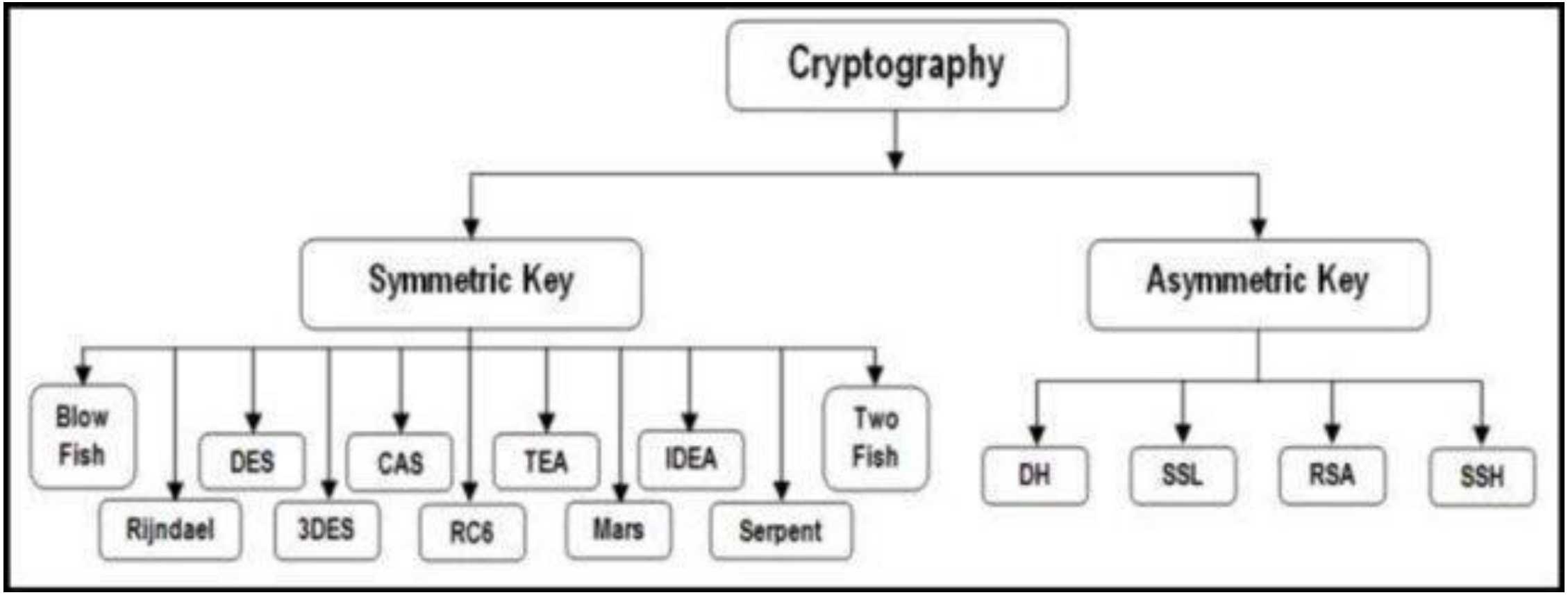
Biner:		Key:		Plainteks:
00010000		X (01011000)		H (01001000)
00001000		M (01001101)		E (01000101)
00001111	XOR	C (01000011)	=	L (01001100)
00000111		K (01001011)		L (01001100)
00000011		L (01001100)		O (01001111)

Kriptografi Symmetric in Daily Life



Sumber gambar: VeePN

Sumber gambar: Kompas



https://www.researchgate.net/figure/Figure-1-Different-Symmetric-Asymmetric-Cryptographic-Algorithms_fig1_318879716

Algoritma Kriptografi Symmetric (Commonly used)

- Blowfish dan Twofish
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)

Kekuatan
Kriptografi Simetris

1. Algoritma simetris lebih cepat dibanding asimetris.
2. Daya komputasi rendah.
3. Keamanan tingkat tinggi.

Kelemahan Kriptografi Simetris

1. Distribusi kunci dalam skala besar sulit.
2. Kebutuhan kunci dalam jumlah besar dari setiap pasang pengguna.
3. Risiko keamanan tinggi karena hanya menggunakan satu kunci.

- Computer Security Principles and Practice Third Edition, William Stallings and Lawrie Brown, Pearson, 2012
- Introduction to computer security, Matt Bishop, Addison Wesley, 2005
- Computer Networking: A Top Down Approach 6th edition Jim Kurose, Keith Ross, and Addison-Wesley
- https://www.ericsson.com/en/blog/2021/7/cryptography-and-privacy-protecting-private-data
- https://selembardigital.com/pelajari-semua-tentang-cryptocurrency-kriptografi-bagaimana-cara-kerjanya/
- https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography/cryptographic-hash-functions
- Katz, J., & Lindell, Y. (2007). Introduction to Modern Cryptography: Principles and Protocols. CRC Press.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson.
- National Institute of Standards and Technology (NIST) - Publications on Secure Hash Standards (SHS)