RSA

ALGORITMA ASIMETRI

Kriptografi – Week 12

RSA

- Ditemukan oleh tiga orang yaitu **R**on Rivest, Adi **S**hamir, dan Leonard **A**dleman yang kemudian disingkat menjadi RSA.
- Termasuk algritma asimetri karena mempunyai dua kunci, yaitu kunci publik dan kunci privat.
- Algoritma kunci-publik yang paling terkenal dan paling banyak aplikasinya.
- Ditemukan oleh tiga peneliti dari MIT (Massachussets Institute of Technology), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976.
- Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

RSA

Pembangkitan pasangan kunci

1. Pilih dua bilangan prima, *a* dan *b* (rahasia)
2. Hitung $n = a.b$ Besaran *n* tidak perlu dirahasiakan.
3. Hitung $\phi(n) = (a - 1)(b - 1)$.
4. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya *e*, yang relatif prima terhadap $\phi(n)$.
5. Hitung kunci dekripsi, *d*, melalui $ed \equiv 1$ (**mod** *m*) atau $d \equiv e^{-1} \bmod (\phi(n))$

Hasil dari algoritma di atas:

- Kunci publik adalah pasangan (*e*, *n*)
- Kunci privat adalah pasangan (*d*, *n*)

Catatan: *n* tidak bersifat rahasia, namun ia diperlukan pada perhitungan enkripsi/dekripsi

RSA

Kunci Publik

- Misalkan a = 47 dan b = 71 (keduanya prima), maka dapat dihitung:

  $n = a \times b = 3337$

  $\phi(n) = (a - 1) \times (b - 1) = 46 \times 70 = 3220$.
- Pilih kunci publik e = 79 (yang relatif prima dengan 3220 karena pembagi bersama terbesarnya adalah 1).
- Hapus a dan b dan kunci publiknya adalah n=3337 dan e=79

Kunci Privat

- Selanjutnya akan dihitung kunci privat d dengan kekongruenan:

$$e \times d \equiv 1 \pmod{m} \Rightarrow \quad d = \frac{1 + (k \times 3220)}{79}$$

Dengan mencoba nilai-nilai k = 1, 2, 3, …, diperoleh nilai d yang bulat adalah 1019. Ini adalah kunci privat (untuk dekripsi).

RSA

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

RSA

- Misalkan plainteks M = HARI INI
  atau dalam ASCII: 726582732737873

  Pecah M menjadi blok yang lebih kecil (misal 3 digit):

  m_1 = 726 m_4 = 273
  m_2 = 582 m_5 = 787
  m_3 = 733 m_6 = 003

  (Perhatikan, m_i masih terletak di dalam antara 0 sampai n – 1)

RSA

- *Enkripsi setiap blok:*

  $c_1 = 726^{79} \bmod 3337 = 215$

  $c_2 = 582^{79} \bmod 3337 = 776$, dst

  Chiperteks C = 215 776 1743 933 1731 158.

- *Dekripsi (menggunakan kunci privat d = 1019)*

  $m_1 = 215^{1019} \bmod 3337 = 726$

  $m_2 = 776^{1019} \bmod 3337 = 582$ dst untuk sisi blok lainnya

  Plainteks M = 726582733273873 yang dalam ASCII karakternya adalah HARI INI.

RSA

- ***Kekuatan dan Keamanan RSA***
  - Kekuatan algoritma *RSA* terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor primanya, yang dalam hal ini $n = a \times b$.
  - Sekali n berhasil difaktorkan menjadi a dan b, maka $\phi(n) = (a - 1)\times(b - 1)$ dapat dihitung. Selanjutnya, karena kunci enkripsi e diumumkan (tidak rahasia), maka kunci dekripsi d dapat dihitung dari persamaan $ed \equiv 1 \pmod{n}$.
  - Penemu algoritma RSA menyarankan nilai a dan b panjangnya lebih dari 100 digit. Dengan demikian hasil kali n = a □ b akan berukuran lebih dari 200 digit.
  - Menurut Rivest dan kawan-kawan, usaha untuk mencari faktor bilangan 200 digit membutuhkan waktu komputasi selama 4 milyar tahun! (dengan asumsi bahwa algoritma pemfaktoran yang digunakan adalah algoritma yang tercepat saat ini dan komputer yang dipakai mempunyai kecepatan 1 milidetik).