

Teori Bilangan

(Bagian 3)

(Update 2023)

Bahan Kuliah IF2120 Matematika Diskrit

Oleh: Rinaldi Munir

Program Studi Teknik Informatika
STEI-ITB



Aplikasi Teori Bilangan

- *ISBN (International Standard Book Number)*
- Fungsi *hash*
- Kriptografi
- Pembangkit bilangan acak-semu

ISBN (International Standard Book Number)

- Kode ISBN terdiri dari 10 angka, biasanya dikelompokkan dengan spasi atau garis, misalnya 0–3015–4561–9.

Catatan: Juga terdapat versi ISBN 13-angka

- ISBN terdiri atas empat bagian kode:
 - kode yang mengidentifikasi negara atau kelompok negara,
 - kode penerbit,
 - kode unik untuk buku tersebut,
 - karakter uji (angka atau huruf X (=10)).



Contoh:



- 1 : kode negara-negara berbahasa Inggris (selain AS)
- 4028 : kode penerbit
- 9462 : kode unik buku yang diterbitkan oleh penerbit
- 7 : karakter uji.

- Misalkan 10 angka ISBN dinyatakan dengan x_1, x_2, \dots, x_{10}
- Kode ISBN memenuhi kekongruenan

$$\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$$

$$(1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + \dots + 10 \cdot x_{10}) \equiv 0 \pmod{11}$$

- Karakter uji dihitung sebagai berikut:

$$\left(\sum_{i=1}^9 ix_i \right) \pmod{11} = \text{karakter uji}$$

- Contoh: ISBN 0–3015–4561–8
 - 0 : kode negara Amerika Serikat
 - 3015 : kode penerbit
 - 4561 : kode unik buku yang diterbitkan
 - 8 : karakter uji.

Kode ISBN ini memenuhi kekongruenan:

$$\begin{aligned}\sum_{i=1}^{10} ix_i &= 1 \cdot 0 + 2 \cdot 3 + 3 \cdot 0 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 4 + 7 \cdot 5 + 8 \cdot 6 + 9 \cdot 1 + 10 \cdot 8 \\ &= 231 \equiv 0 \pmod{11}\end{aligned}$$

Karakter uji ini didapatkan sebagai berikut:

$$\begin{aligned}\sum_{i=1}^9 ix_i &= 1 \cdot 0 + 2 \cdot 3 + 3 \cdot 0 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 4 + 7 \cdot 5 + 8 \cdot 6 + 9 \cdot 1 \\ &= 151\end{aligned}$$

Jadi, karakter ujinya adalah $151 \bmod 11 = 8$.

Latihan 1

Sebuah buku terbitan September 2018 memiliki ISBN $9p7-2309-97$. Tentukan nilai p dan karakter uji dari nomor ISBN tersebut jika diketahui $3p \equiv 2 \pmod{5}$.

Jawaban:

- $3p \equiv 2 \pmod{5} \rightarrow 3p = 2 + 5k \rightarrow p = (2 + 5k)/3$ untuk k sembarang bilangan bulat

Untuk nilai $k =$

$$k = 1 \rightarrow p = 2/3$$

$$k = 2 \rightarrow p = 4$$

$$k = 3 \rightarrow p = 17/3$$

$$k = 4 \rightarrow p = 22/3$$

$$k = 5 \rightarrow p = 9$$

$$k = 6 \rightarrow p = 32/3$$

$$k = 7 \rightarrow p = 37/3$$

$$k = 8 \rightarrow p = 14$$

...dst

- Dapat dilihat di atas, untuk $k = 2, 5, 8, \dots$ nilai p bulat, namun untuk kode ISBN nilai p harus dalam rentang bilangan bulat 0-9, jadi nilai p yang memenuhi adalah **4** dan **9**.

Untuk mencari karakter uji, diketahui

$$\sum_{i=1}^9 ix_i \bmod 11 = \text{karakter uji}$$

Karakter uji untuk kode ISBN 947-2309-97 dapat dicari sebagai berikut :

$$\sum_{i=1}^9 ix_i = (1)(9) + (2)(4) + (3)(7) + (4)(2) + (5)(3) + (6)(0) + (7)(9) + (8)(9) + (9)(7) = 259$$

Jadi karakter uji untuk ISBN di atas = $259 \bmod 11 = 6 \rightarrow 947-2309-97-6$

Karakter uji untuk kode ISBN 997-2309-97 dapat dicari sebagai berikut :

$$\sum_{i=1}^9 ix_i = (1)(9) + (2)(9) + 3(7) + (4)(2) + (5)(3) + 6(0) + (7)(9) + (8)(9) + (9)(7) = 269$$

Jadi karakter uji untuk ISBN di atas = $269 \bmod 11 = 5 \rightarrow 997-2309-97-5$

Latihan (Kuis 2020)

Sebuah buku memiliki kode ISBN 0-30X5-4561-Y dan memenuhi $3X \bmod 11 = 1$, serta Y adalah karakter uji. Tentukan semua pasangan X dan Y yang mungkin.

(Jawaban pada halaman berikut)

Jawaban:

Pertama, cari terlebih dahulu X nya

$$3X = 1 + 11n$$

$$X = (1 + 11n) / 3$$

Karena X haruslah bilangan bulat < 10, maka X yang memenuhi adalah 4.

Setelah itu kita cari Y nya. Karena Y adalah karakter uji, maka berlaku

$$(\sum_{i=1}^9 i \cdot a_i) \bmod 11 = Y$$

maka

$$(1 \cdot 0 + 2 \cdot 3 + 3 \cdot 0 + 4 \cdot 4 + 5 \cdot 5 + 6 \cdot 4 + 7 \cdot 5 + 8 \cdot 6 + 9 \cdot 1) \bmod 11 = 163 \bmod 11 = 9$$

Sehingga $Y = 9$

Jadi pasangan X dan Y yang memenuhi adalah $X = 4$ dan $Y = 9$

Fungsi *Hash*

- Kegunaan: pengalamatan data di dalam memori untuk tujuan pengaksesan data dengan cepat.
- Bentuk: $h(K) = K \bmod m$
 - m : jumlah lokasi memori yang tersedia
 - K : kunci (*integer*)
 - $h(K)$: lokasi memori untuk data dengan kunci unik K

Contoh: data record mahasiswa, NIM adalah kunci (*K*)

NIM	Nama	MatKul	Nilai
13598011	Amir	Matematika Diskrit	A
13598012	Bonar	Arsitektur Komputer	B
13598014	Santi	Algoritma	D
13598015	Irwan	Algoritma	C
13598017	Rahman	Struktur Data	C
13598018	Ismu	Arsitektur Komputer	B
13598019	Tommy	Algoritma	E
13598021	Cecep	Algoritma	B
13598023	Badru	Arsitektur Komputer	B
13598025	Hamdan	Matematika Diskrit	B
13598027	Rohadi	Algoritma	A
13598028	Hans	Struktur Data	C
13598029	Maman	Arsitektur Komputer	B

Contoh: $m = 11$ mempunyai sel-sel memori yang diberi indeks 0 sampai 10. Akan disimpan data *record* yang masing-masing mempunyai kunci 15, 558, 32, 132, 102, dan 5.

$$h(15) = 15 \bmod 11 = 4$$

$$h(558) = 558 \bmod 11 = 8$$

$$h(32) = 32 \bmod 11 = 10$$

$$h(132) = 132 \bmod 11 = 0$$

$$h(102) = 102 \bmod 11 = 3$$

$$h(5) = 5 \bmod 11 = 5$$

132			102	15	5			558		32
0	1	2	3	4	5	6	7	8	9	10

- Kolisi (*collision*) terjadi jika fungsi *hash* menghasilkan nilai *h* yang sama untuk *K* yang berbeda.
- Jika terjadi kolisi, cek elemen berikutnya yang kosong.

Contoh: $K = 74 \rightarrow h(74) = 74 \bmod 11 = 8$

132			102	15	5			558		32
0	1	2	3	4	5	6	7	8	9	10

Oleh karena elemen pada indeks 8 sudah berisi 558, maka 74 ditaruh pada elemen kosong berikutnya: 9

132			102	15	5			558	74	32
0	1	2	3	4	5	6	7	8	9	10

- Fungsi *hash* juga digunakan untuk *me-locate* elemen yang dicari.

Misalkan akan dicari data dengan nilai $K = 102$

Posisi 102 di dalam larik dihitung dengan fungsi *hash* $\rightarrow h(102) = 102 \bmod 11 = 3$

132			102	15	5			558	74	32
0	1	2	3	4	5	6	7	8	9	10



Misalkan akan dicari data dengan nilai $K = 214$

Posisi 214 di dalam larik dihitung dengan fungsi *hash* $\rightarrow h(214) = 214 \bmod 11 = 5$

Karena pada sel dengan indeks 5 bukan berisi 214, maka disimpulkan $K = 214$ tidak ditemukan di dalam larik.

Latihan 2

Sebuah area parkir mempunyai sejumlah *slot* atau *space* yang dinomori 0 sampai 25. Mobil yang hendak parkir di area tersebut ditentukan dengan sebuah fungsi *hash*. Fungsi *hash* tersebut menentukan nomor *slot* yang akan ditempati mobil yang hendak parkir berdasarkan 3 angka terakhir pada plat nomor polisinya.

- (a) Tentukan fungsi *hash* yang dimaksudkan.
- (b) Tentukan nomor *slot* yang ditempati mobil yang datang berturut-turut dengan plat nomor polisinya adalah 423251, 76540, 17121, 2310, 4124, 1102, 1724

- Jawaban:

(a) $h = x \bmod 26$

(b) $423251 \rightarrow 3 \text{ angka terakhir} = 251 \rightarrow 251 \bmod 26 = 17$ (slot 17)

$76540 \rightarrow 3 \text{ angka terakhir} = 540 \rightarrow 540 \bmod 26 = 20$ (slot 20)

$17121 \rightarrow 3 \text{ angka terakhir} = 121 \rightarrow 121 \bmod 26 = 17$ (tetapi slot nomor 17 sudah terisi, jadi isi slot kosong berikutnya, yaitu 18)

$2310 \rightarrow 3 \text{ angka terakhir} = 310 \rightarrow 310 \bmod 26 = 24$ (slot 24)

$4124 \rightarrow 3 \text{ angka terakhir} = 124 \rightarrow 124 \bmod 26 = 20$ (slot 21 karena slot 20 sudah terisi)

$1102 \rightarrow 3 \text{ angka terakhir} = 102 \rightarrow 102 \bmod 26 = 24$ (slot 25 karena slot 24 sudah terisi)

$1724 \rightarrow 3 \text{ angka terakhir} = 724 \rightarrow 724 \bmod 26 = 22$ (slot 22)

Jadi, mobil-mobil yang datang mengisi slot 17, 20, 18, 24, 21, 25, dan 22

Latihan (Kuis 2021)

Dalam rangka mata kuliah olahraga, seluruh mahasiswa Universitas Sukamatdis dari K02 mata kuliah olahraga diminta untuk membentuk 7 barisan. Barisan ini dinomori dari nomor 1 sampai 7 (**Perhatikan**: nomor urut dimulai dari 1, bukan dari 0). Barisan yang dimasuki oleh seorang mahasiswa ditentukan dengan sebuah fungsi hash. Fungsi hash tersebut menentukan nomor barisan yang dimasuki tiap mahasiswa berdasarkan 3 angka terakhir dari NIM mahasiswa tersebut.

- a. Tentukan fungsi hash(h) untuk penentuan barisan yang dimasuki setiap mahasiswa.
- b. Misalkan setiap barisan hanya boleh diisi oleh 2 mahasiswa saja, tentukan barisan yang ditempati mahasiswa-mahasiswa yang memasuki barisan secara berturut-turut dengan NIM 13519096, 13217031, 16519011, 18218157, 10818013, 10517112, 10219024, 13816194, 16219242. Asumsi barisan kosong dan jika barisan sudah penuh, mahasiswa memasuki barisan setelahnya.

Jawaban:

a. Terdapat 7 barisan dengan penomoran 1 sampai 7. Maka fungsi hash yang didapat adalah $h = (x \bmod 7) + 1$, dengan x berupa nomor barisan.

b.

13519096 -> 3 angka terakhir = 96 -> $(96 \bmod 7) + 1 = 6$

13217031 -> 3 angka terakhir = 31 -> $(31 \bmod 7) + 1 = 4$

16519011 -> 3 angka terakhir = 11 -> $(11 \bmod 7) + 1 = 5$

18218157 -> 3 angka terakhir = 157 -> $(157 \bmod 7) + 1 = 4$

10818013 -> 3 angka terakhir = 13 -> $(13 \bmod 7) + 1 = 7$

10517112 -> 3 angka terakhir = 112 -> $(112 \bmod 7) + 1 = 1$

10219024 -> 3 angka terakhir = 24 -> $(24 \bmod 7) + 1 = 4$, namun barisan 4 sudah penuh maka memasuki barisan selanjutnya yaitu barisan 5.

13816194 -> 3 angka terakhir = 194 -> $(194 \bmod 7) + 1 = 6$

16219242 -> 3 angka terakhir = 242 -> $(242 \bmod 7) + 1 = 5$, namun barisan 5 sudah penuh, barisan selanjutnya yaitu barisan 6 juga sudah penuh, maka memasuki barisan selanjutnya yaitu barisan 7.

Kriptografi



- Dari Bahasa Yunani yang artinya “*secret writing*”
- **Kriptografi** adalah ilmu dan seni untuk menjaga keamanan pesan dengan cara menyandikannya menjadi bentuk lain yang tidak bermakna.
- Tujuan: agar pesan yang bersifat rahasia tidak dapat dibaca oleh pihak yang tidak berhak.

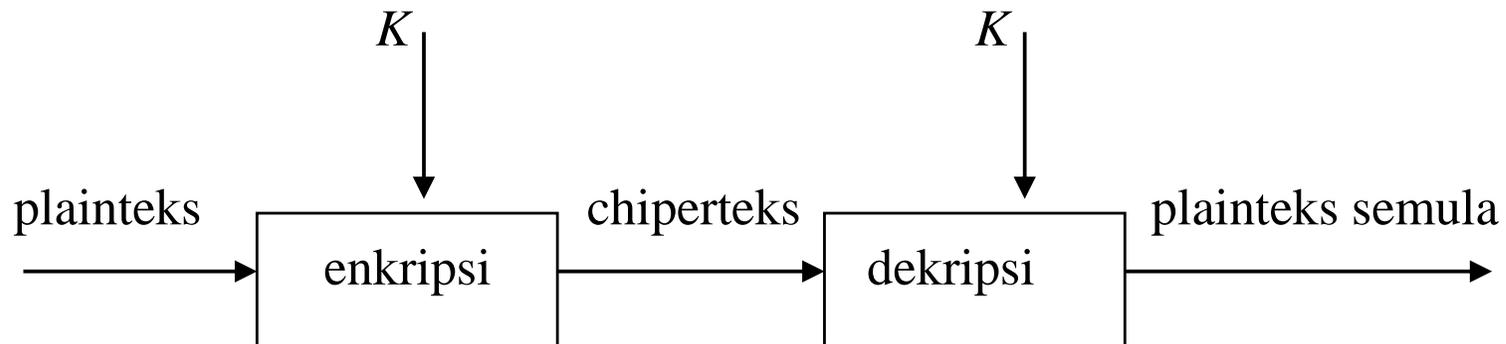
- **Pesan:** data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain: **plainteks** (*plaintext*)
- **Cipherteks** (*ciphertext*): pesan yang telah disandikan sehingga tidak memiliki makna lagi.

Contoh:

Plainteks: culik anak itu jam 11 siang

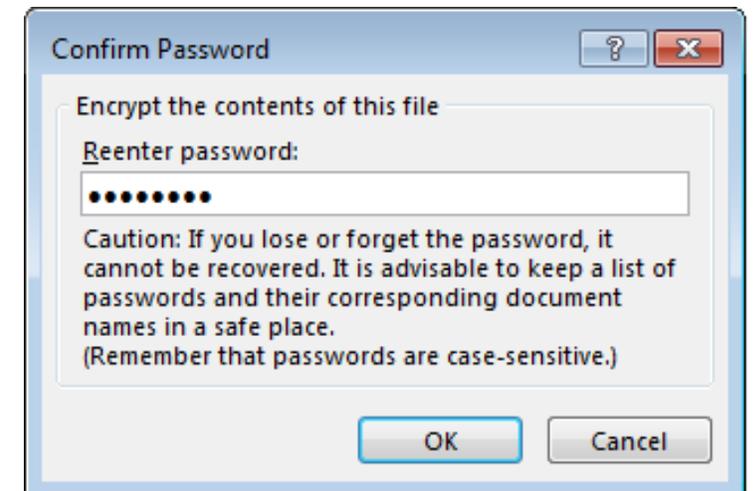
Cipherteks: t^\$gfUi9rewoFpfdWqL: [uTcxZy

- **Enkripsi** (*encryption*): proses menyandikan plainteks menjadi cipherteks.
- **Dekripsi** (*decryption*): Proses mengembalikan cipherteks menjadi plainteksnya.



Aplikasi Enkripsi-Dekripsi

1. Pengiriman data melalui saluran komunikasi (*data encryption on motion*).
→ pesan dikirim dalam bentuk cipherteks
2. Penyimpanan dokumen di dalam *disk storage* (*data encryption at rest*)
→ data disimpan di dalam *disk* dalam bentuk cipherteks



Contoh enkripsi pada dokumen

Plainteks (plain.txt):

```
Ketika saya berjalan-jalan di pantai,  
saya menemukan banyak sekali kepiting  
yang merangkak menuju laut. Mereka  
adalah anak-anak kepiting yang baru  
menetas dari dalam pasir. Naluri  
mereka mengatakan bahwa laut adalah  
tempat kehidupan mereka.
```

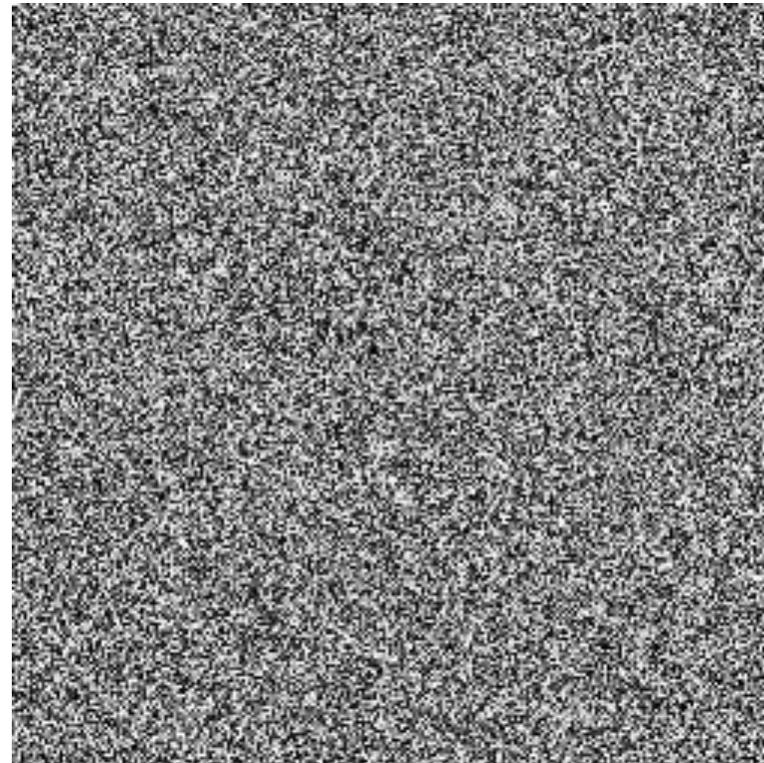
Cipherteks (cipher.txt):

```
Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/□p}âpx;  
épêp/|t}t|âzp}/qp}êpz/étzp{x/zt□xâx  
}v êp}v/|tüp}vzpz/|t}âyä/{pââ=/\tütz  
p psp{pw/p}pz<p}pz/zt□xâx}v/êp}  
v/qpüâ |t}tâpé/spüx/sp{p|/□péxü=/  
p{âüx |ttüzp/|t}vpâpzp}/qpwâp/{pââ  
/psp{pw ât|□pâ/ztwxsä□p}/|tützp=
```

Plainteks (lena.bmp):



Cipherteks (lena2.bmp):



Plainteks (siswa.dbf):

NIM	Nama	Tinggi	Berat
000001	Elin Jamilah	160	50
000002	Fariz RM	157	49
000003	Taufik Hidayat	176	65
000004	Siti Nurhaliza	172	67
000005	Oma Irama	171	60
000006	Aziz Burhan	181	54
000007	Santi Nursanti	167	59
000008	Cut Yanti	169	61
000009	Ina Sabarina	171	62

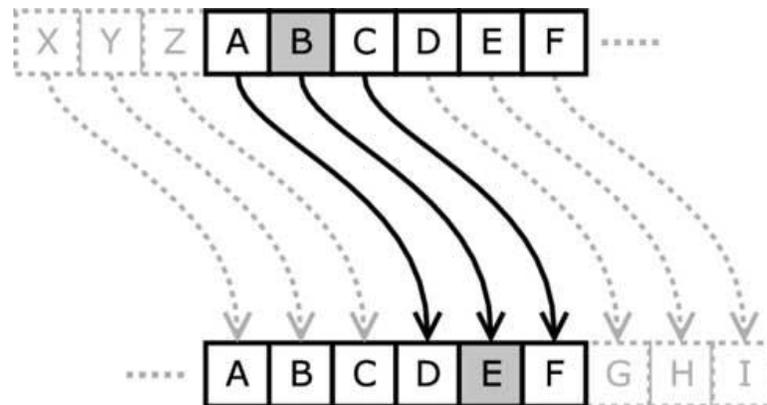
Cipherteks (siswa2.dbf):

NIM	Nama	Tinggi	Berat
000001	tüp}vzpz/ t}äyâ/{ää	äzp}	épêp
000002	t}tâpé/spüx/sp	péxü=	ztwxsä□
000003	ât □pâ/ztwxsä□p}/	}/ tü	spüx/
000004	épêp/ t}t äzp}/qpêpz	qp}êpz	wxsä
000005	étzp{x/zt□xâx}v êp}	pää/psp	étzp{
000006	spüx/sp{p /□péxü=/}	xâx}v	ttüzp/
000007	Ztâxzp/épêp/qtüypp}<	äzp}	}äyâ/{
000008	qpwâp/{pää/psp{pw	Ztwxs	xâx}v
000009	}t äzp}/qp}êpz/ép{	qp}êp	äzp}/qp

Keterangan: hanya *field* Nama, Berat, dan Tinggi yang dienkrpsi.

Caesar Cipher

- Algoritma enkripsi sederhana pada masa raja Julius Caesar
- Tiap huruf alfabet digeser 3 huruf ke kanan secara *wrapping*



Contoh: Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

Copyright (c) 1999 Les Editions Albert René / Goscinny-Uderzo



- Misalkan setiap huruf dikodekan dengan angka:

$$A = 0, B = 1, C = 2, \dots, Z = 25$$

Misalkan huruf plainteks dinyatakan sebagai p dan huruf cipherteks sebagai c , maka secara matematis enkripsi dan dekripsi pada Caesar *cipher* dinyatakan dengan persamaan modulo berikut:

$$\text{Enkripsi: } c = E(p) = (p + 3) \bmod 26$$

$$\text{Dekripsi: } p = D(c) = (c - 3) \bmod 26$$

Contoh:

Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBD REHOLA**

Enkripsi:

$$p_1 = 'A' = 0 \quad \rightarrow c_1 = E(0) = (0 + 3) \bmod 26 = 3 \bmod 26 = 3 = 'D'$$

$$p_2 = 'W' = 22 \quad \rightarrow c_2 = E(22) = (22 + 3) \bmod 26 = 25 \bmod 26 = 25 = 'Z'$$

$$p_3 = 'A' = 0 \quad \rightarrow c_3 = E(0) = (0 + 3) \bmod 26 = 3 \bmod 26 = 3 = 'D'$$

$$p_4 = 'S' = 18 \quad \rightarrow c_4 = E(18) = (18 + 3) \bmod 26 = 21 \bmod 26 = 21 = 'V'$$

dst...

Dekripsi:

$$c_1 = 'D' = 3 \quad \rightarrow p_1 = D(3) = (3 - 3) \bmod 26 = 0 \bmod 26 = 0 = 'A'$$

$$c_2 = 'Z' = 25 \quad \rightarrow p_2 = D(25) = (25 - 3) \bmod 26 = 22 \bmod 26 = 22 = 'W'$$

$$c_3 = 'D' = 3 \quad \rightarrow p_3 = D(3) = (3 - 3) \bmod 26 = 0 \bmod 26 = 0 = 'D'$$

$$c_4 = 'V' = 21 \quad \rightarrow p_4 = D(21) = (21 - 3) \bmod 26 = 18 \bmod 26 = 18 = 'S'$$

dst..

- Jika pergeseran huruf sejauh k , maka:

$$\text{Enkripsi: } \mathbf{c = E(p) = (p + k) \bmod 26}$$

$$\text{Dekripsi: } \mathbf{p = D(c) = (c - k) \bmod 26}$$

k = kunci rahasia

- Pada *Caesar Cipher*, $k = 3$

- Untuk alfabet ASCII 256 karakter,

$$\text{Enkripsi: } \mathbf{c = E(p) = (p + k) \bmod 256}$$

$$\text{Dekripsi: } \mathbf{p = D(c) = (c - k) \bmod 256}$$

Latihan 3

Salah satu program enkripsi di dalam sistem operasi *Linux* adalah **ROT13**. Enkripsi dilakukan dengan mengganti sebuah huruf dengan huruf ke-13 berikutnya dari susunan alfabet.

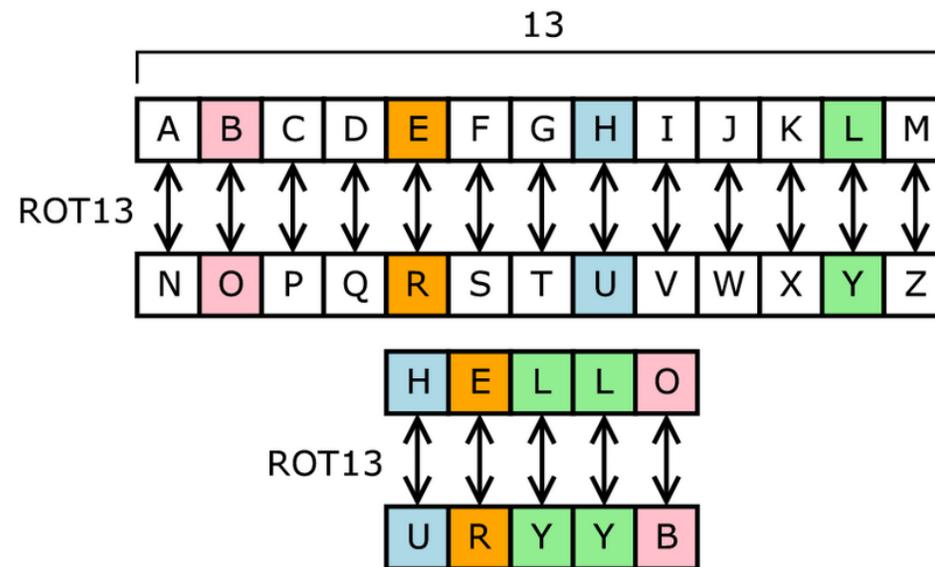
- (a) Nyatakan fungsi enkripsi dan dekripsi di dalam ROT13 sebagai persamaan aritmetika modulo dalam p dan c .
- (b) Jika enkripsi dilakukan dua kali berturut-turut terhadap plainteks, apa yang terjadi?

Jawaban:

a) $c = E(p) = (p + 13) \text{ mod } 26$

$p = D(c) = (c - 13) \text{ mod } 26$

b) Jika dilakukan 2 kali enkripsi terhadap *plaintext*, maka hasilnya sama dengan *plaintext* awal.



Latihan (Kuis 2022)

Panitia SPARTA HMIF berencana untuk membuat sebuah rangkaian puzzle yang harus dipecahkan oleh calon anggota HMIF. Salah satu puzzle tersebut adalah diberikan adalah dekripsi sandi untuk masuk ke dalam *zoom meeting*. Sandi dienkripsi menggunakan teknik caesar *cypher* dengan mengganti karakter sandi ke-12 berikutnya . Karakter pada sandi dapat berisi angka (0–9) atau huruf kapital (A–Z). Angka dikodekan sesuai dengan nilai angka tersebut sedangkan huruf dikodekan sesuai urutan huruf pada alfabet ditambah 10 (A = 0+10, B=1+10, Z=25+10). Dari deskripsi diatas jawablah pertanyaan dibawah ini,

- a) Nyatakan fungsi enkripsi dan dekripsi pada permasalahan diatas sebagai persamaan aritmetika modulo dalam p dan c.
- b) Bantu calon peserta HMIF untuk mendekripsi sandi “BFW3QX5G” tanpa tanda petik dua.

Jawaban:

$$\begin{aligned} \text{a) } c &= E(p) = (p + 12) \bmod 36 \\ p &= D(c) = (c - 12) \bmod 36 \end{aligned}$$

b)

0	1	2	3	4	5	6	7	8	9	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
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	A	B

$$B \rightarrow (11-12) \bmod 36 = 35 \rightarrow Z$$

$$F \rightarrow 3$$

$$W \rightarrow K$$

$$3 \rightarrow R$$

$$Q \rightarrow E$$

$$X \rightarrow L$$

$$5 \rightarrow T$$

$$G \rightarrow 4$$

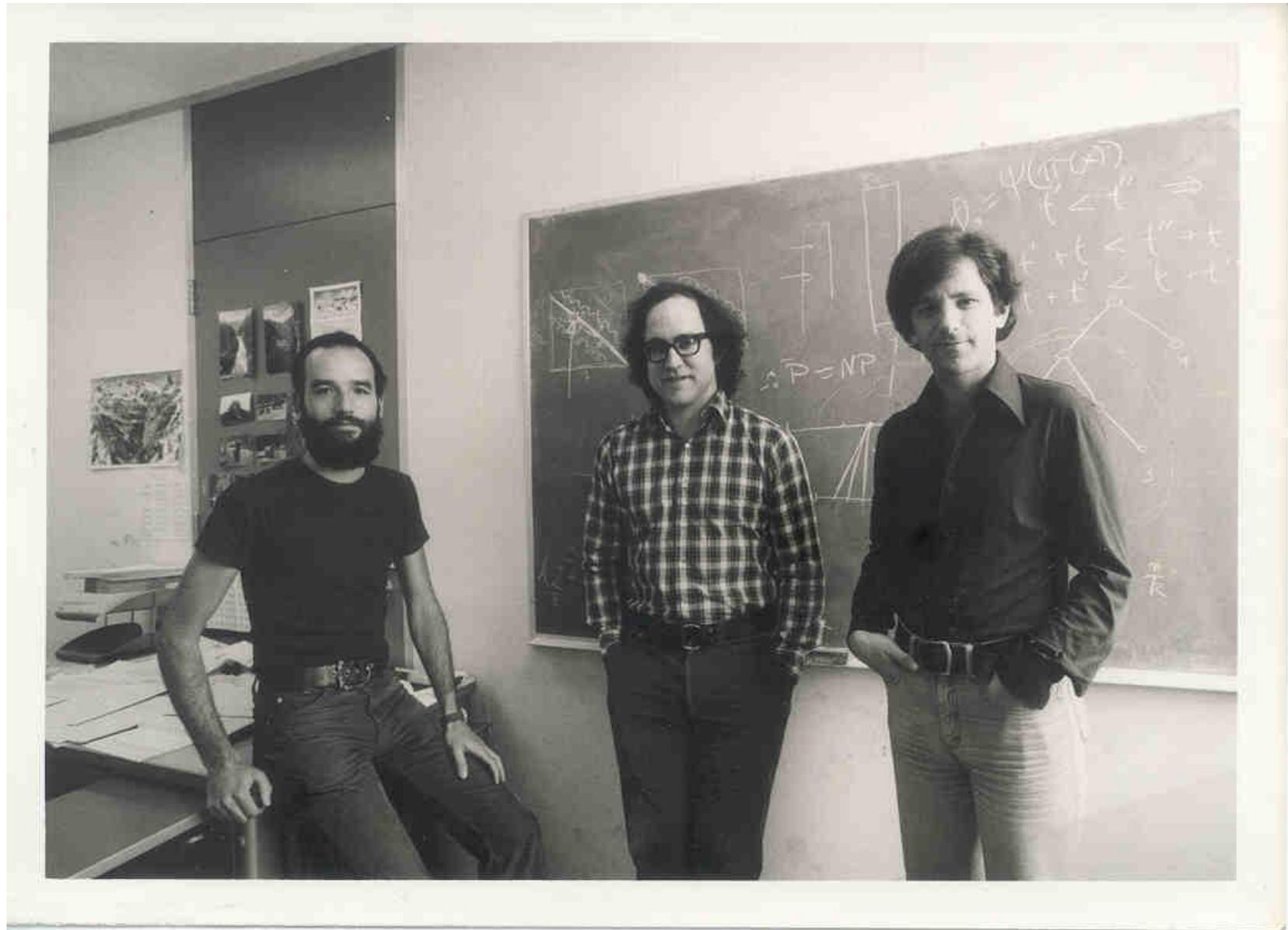
Hasil: Z3KRELT4

Algoritma RSA

- Dibuat oleh tiga peneliti dari *MIT (Massachusetts Institute of Technology)*, yaitu Ronald Rivest, Adi Shamir, dan Leonard Adleman, pada tahun 1976.

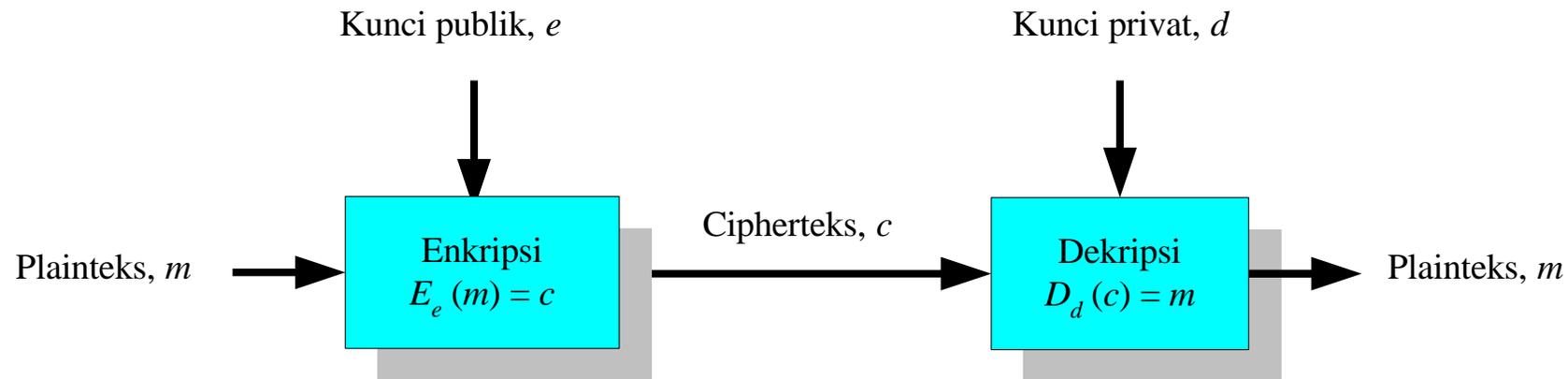


- Termasuk algoritma **kriptografi asimetri**.
- Asimetri: kunci untuk enkripsi berbeda dengan kunci untuk dekripsi



Rinaldi M/IF2120 Matematika Diskrit

- Di dalam Algoritma RSA, setiap pengguna memiliki sepasang kunci:
 1. Kunci publik, e : untuk mengenkripsi pesan
 2. Kunci privat, d : untuk mendekripsi pesan



- Kunci publik tidak rahasia (diumumkan kepada publik), sedangkan kunci privat rahasia, hanya diketahui oleh pemilik kunci.
- Dinamakan juga **kriptografi kunci-public** (*public-key cryptography*)

Prosedur pembangkitan pasangan kunci di dalam RSA

1. Pilih dua bilangan prima, p dan q (rahasia)
2. Hitung $n = pq$. Besaran n tidak perlu dirahasiakan.
3. Hitung $m = (p - 1)(q - 1)$. (rahasia)
4. Pilih sebuah bilangan bulat untuk kunci publik, e , yang relatif prima terhadap m , yaitu $\text{PBB}(e, m) = 1$.
5. Hitung kunci dekripsi, d , melalui kekongruenan $ed \equiv 1 \pmod{m}$.

- **Contoh.** Misalkan $p = 47$ dan $q = 71$ (keduanya prima), maka dapat dihitung

$$n = pq = 47 \cdot 71 = 3337$$

$$m = (p - 1)(q - 1) = 3220.$$

Pilih kunci publik $e = 79$ (yang relatif prima dengan 3220), yaitu.

Nilai e dan n dapat dipublikasikan ke umum.

- **Catatan:** Dalam praktek, nilai p , q , dan e adalah bilangan yang sangat besar (minimal 200 digit)

- Selanjutnya dihitung kunci dekripsi d dengan kekongruenan:

$$ed \equiv 1 \pmod{m}$$

yang dapat dihitung dengan

$$d = \frac{1+km}{e} = \frac{1+3220k}{79}$$

dengan mencoba $k = 0, 1, 2, \dots$, diperoleh nilai d bilangan bulat adalah

$$d = 1019$$

Ini adalah kunci dekripsi.

Prosedur enkripsi-dekripsi:

Enkripsi: $p^e \equiv c \pmod{n}$ atau dapat ditulis: $c = p^e \bmod n$

Dekripsi: $c^d \equiv p \pmod{n}$ atau dapat ditulis: $p = c^d \bmod n$

- Misalkan plainteks: 'HARI INI'

atau dalam desimal ASCII: 7265827332737873

Pecah pesan menjadi blok yang lebih kecil (misal 3-angka) untuk memudahkan komputasi:

$$p_1 = 726$$

$$p_2 = 582$$

$$p_3 = 733$$

$$p_4 = 273$$

$$p_5 = 787$$

$$p_6 = 003$$

- *Enkripsi setiap blok (menggunakan kunci publik $e = 79$)* : $c = p^e \bmod n$

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

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

dst untuk sisa blok lainnya

Luaran: chiperteks $C = 215\ 776\ 1743\ 933\ 1731\ 158$.

- *Dekripsi (menggunakan kunci privat $d = 1019$)*: $p = c^d \bmod n$

$$p_1 = 215^{1019} \bmod 3337 = 726$$

$$p_2 = 776^{1019} \bmod 3337 = 582$$

dst untuk sisi blok lainnya

Luaran: plainteks = 7265827332737873

atau dalam kode ASCII karakternya adalah HARI INI.

Pembangkit Bilangan Acak

- Pembangkit bilangan acak yang berbasis kekongruenan linjar adalah *linear congruential generator* atau *LCG*:

$$X_n = (aX_{n-1} + b) \bmod m$$

X_n = bilangan acak ke- n dari deretnya

X_{n-1} = bilangan acak sebelumnya

a = faktor pengali

b = *increment*

m = modulus

Kunci pembangkit adalah X_0 yang disebut **umpan** (*seed*).

Contoh: $X_n = (7X_{n-1} + 11) \bmod 17$, dan $X_0 = 0$

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

Latihan soal teori bilangan

(diambil dari soal kuis dan UAS)

1. Dengan menggunakan Teorema Fermat, hitunglah $(5^{2017} \bmod 7 + 5^{2017} \bmod 11) \bmod 7$. **(Nilai: 10)**
2. (a) Hitunglah $51^{-1} \pmod{1008}$
(b) Gunakan hasil jawaban a di atas untuk menemukan semua solusi bilangan bulat x yang memenuhi kongruensi $51x \equiv 177 \pmod{1008}$
3. Sebuah buku memiliki kode ISBN **0-1p026-690-q**. Tentukan nilai $(p + q) \bmod 3$ dari nomor ISBN tersebut jika diketahui $6p \equiv 3 \pmod{7}$

4. (a) Carilah PBB (atau *gcd*) dari 621 dan 483
 (b) Cari solusi dari $621m + 483n = k$, dimana k adalah PBB dari 621 dan 483
 (c) Hitung $3^{64} \bmod 67$ dengan menggunakan Fermat's Theorem
5. Berapakah nilai x dan y bilangan bulat yang memenuhi persamaan $1757x - 1631y = 483$?
6. Salah satu penggunaan *Chinese Remainder Problem* adalah *Secret sharing* yang merupakan salah satu metode kriptografi. Misal terdapat sebuah rahasia S , maka rahasia tersebut dibagi menjadi beberapa bagian (*shares*). Rahasia S dapat dibangun kembali hanya jika seseorang memiliki set *shares* yang valid. Salah satu implementasi *secret sharing* adalah skema **Asmuth-Bloom**. Rahasia S akan dibagi ke dalam beberapa $I_0, I_1, I_2, \dots, I_n$ *shares*. Bagian terakhir dari skema ini adalah mendapatkan nilai S dengan persamaan $S = x_0 \bmod p_0$, p_0 adalah sebuah bilangan yang ditentukan saat pembagian *shares*. Kemudian, diberikan sebuah baris bilangan m_0, m_1, \dots, m_k yang masing-masing saling relatif prima, maka x_0 merupakan solusi unik modulo $(m_0 \cdot m_1 \cdot m_2 \cdot \dots \cdot m_n)$ dari persamaan: **(Nilai = 25)**

$$x \equiv I_1 \bmod m_1, x \equiv I_2 \bmod m_2, x \equiv I_3 \bmod m_3, \dots, x \equiv I_n \bmod m_n$$

Untuk $p_0 = 5$, $\{(I_k, m_k)\} = \{(1,7), (9,11), (5,13)\}$, tentukan nilai rahasia dari *secret sharing* !

TAMAT