Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Solusi Ujian Tengah Semester **IF4020 Kriptografi**
Senin, 21 Oktober 2025
Waktu: 100 menit
Dosen: Dr. Ir. Rinaldi, M.T

Berdoalah terlebih dahulu agar Anda berhasil dalam mengerjakan ujian ini!

1. **(Nilai=10)** Diketahui suatu cipherteks dengan *Caesar Cipher* seperti berikut "rfc ambc dmp rfc lcvr kccrgle gq gltglagzjc". Coba pecahkan cipherteks di atas dan sebutkan kuncinya.

Jawaban:
Salah satu caranya adalah coba dekripsi cipherteks tersebut dengan k = 1, 2, 3, … dst sampai ketemu pesan bermakna

k = 1 → qeb zlab clo qeb kbuq jbbqfkd fp fksfkzfyib
k = 2 → pda ykza bkn pda jatp iaapejc eo ejrejyexha
k = 3 → ocz xjyz ajm ocz izso hzzodib dn diqdixdwgz
…
k = 24 → the code for the next meeting is invincible

Jadi, k = 24 dan plainteks adalah "the code for the next meeting is invincible"

2. **(Nilai = 5)** Sebuah gambar berukuran 2 x 4 dienkripsi, sehingga nilai-nilai pixelnya (0 sampai 3) menjadi sebagai berikut:

1	0	0	3
2	3	1	3

Hitung entropi gambar hasil enkripsi

Jawaban:
Rumus entropi:

$$H(X) = -\sum_{i=1}^{n} p(x_i)\ \log_2\ p(x_i)$$

n = 4 (yaitu huruf 0, 1, 2, 3)
p(0) = 2/8 = 0.25, p(1) = 2/8 = 0.25, p(2) = 1/8 = 0.125, p(3) = 3/8 = 0.375

H(x) = −[0.25 $\log_2$(0.25) + 0.25 $\log_2$(0.25) + 0.125 $\log_2$(0.125) + 0.375 $\log_2$(0.375) = 1.905625

Jadi, entropi citra tersebut = 1.906 bit

3. **(Nilai = 10)** Sebuah pesan mula-mula dienkripsi dengan cipher transposisi (lebar kolom = 6), selanjutnya hasilnya dienkripsi lagi dengan Vigenere Cipher dengan kata kunci = "CIPETESELATAN", hasil akhirnya adalah cipherteks berikut:

KUSRXWSERSBSZCBAENRSEXDISUWMGM

Dekripsi Kembali cipherteks di atas menjadi plainteks (Tabel Vigenere terlampir)

Jawaban:

Cipherteks: KUSRXWSERSBSZCBAENRSEXDISUWMGM

Dekripsi: mula-mula dekripsi terlebih dahulu dengan Vigenere Cipher menggunakan kunci CIPETESELATAN, hasilnya:

IMDNESAAGSISMATLAUNAAMDPSHUERI

Selanjutnya dekripsi lagi hasil tersebut dengan cipher transposisi,
dengan ukuran kolom = panjang cipherteks/6 = 30/6 = 5

Susun menjadi 5 kolom:

```
IMDNE
SAAGS
ISMAT
LAUNA
AMDPS
HUERI
```

Baca per kolom, hasilnya: ISILAH MASA MUDAMU DENGAN PRESTASI

4. **(Nilai = 10)** Diketahui sebuah gambar (image) berwarna berformat bitmap berukuran 2800 x 1600 pixel. Setiap pixel berukuran 3 byte (format RGB).
   (a) Jika dilakukan penyisipan pesan dengan metode LSB 1-bit ke dalam gambar tersebut, berapa ukuran maksimal pesan yang dapat disembunyikan di dalam gambar dalam satuan byte dan Kilobyte?
   (b) Apakah file berukuran 1500 KB dapat disisipkan ke dalam file gambar tersebut jika penyisipan pesan dilakukan pada 2-bit LSB?

Jawaban:

Jumlah pixel = 2800 x 1600 = 4.480.000 pixel
Jumlah byte = 4.480.000 x 3 byte = 13.440.000 byte

(a) Satu byte dapat disisipkan 1 bit pesan, maka jumlah bit yang dapat disisipkan maksimal adalah
13.440.000 bit = 13.440.000/8 = 1.680.000 byte = 1.680.000/1024 = 1.640,625 KB
Catatan: 1 KB = 1024 byte

(b) Satu byte dapat disisipkan 2 bit pesan, maka jumlah bit yang dapat disisipkan maksimal adalah
13.440.000 x 2 bit = 26.880.000 bit = 26.880.000/8 = 3.360.000 byte = 3.360.000/1024 = 3.281,25 KB
Oleh karena pesan berukuran 1500 KB < 3.281,25 KB, maka file dapat disisipkan ke dalam file gambar

5. **(Nilai = 10)** Pecahkan Affine Cipher jika diketahui bigram yang paling sering muncul di dalam cipherteks adalah JP. Lalu dekripsilah trigram 'IZW' (ini adalah trigram yang sering muncul di dalam teks Bahasa Inggris). Semua pesan dalam Bahasa Inggris. Gunakan pengkodean karakter: A = 0, B = 1, C = 2, …, Y = 24, Z = 25

Jawaban:

Affine cipher

Enkripsi: $C \equiv mP + b \pmod n$

Dekripsi: $P \equiv m^{-1} (C - b) \pmod n$

Bigram yang paling sering muncul, terka TH

$T \rightarrow J$ (T = 19, J = 9)

$H \rightarrow P$ (H = 7, P = 15)

Persamaan kekongruenan:

$15 \equiv 7m + b \pmod{26}$

$9 \equiv 19m + b \pmod{26}$ -

$6 \equiv -12m \pmod{26} \rightarrow -6 \equiv 12m \pmod{26} \rightarrow 20 \equiv 12m \pmod{26} \rightarrow m \equiv 6 \pmod{26}$

Oleh karena 6 dan 26 tidak relatif prima, makai m = 6 tidak dapat digunakan di dalam affine cipher
Namun, kita dapat menyatakan $20 \equiv 12m \pmod{26}$ ekivalen dengan $10 \equiv 6m \pmod{13}$ dengan cara membagi 2 kedua ruas termasuk modusnya, sehingga $m \equiv 6 \pmod{13}$

Nilai m = 6 tidak dapat digunakan (karena tidak relative prima dengan 26), namun nilai berikutnya dalam modulus 13 adalah m = 19 karena $19 \equiv 6 \pmod{13}$. Jadi, m = 19

Substitusikan m = 19 ke dalam $9 \equiv 19m + b \pmod{26}$:

$9 \equiv 19(19) + b \pmod{26}$
$9 \equiv 361 + b \pmod{26}$
$9 \equiv 23 + b \pmod{26}$
$-14 \equiv b \pmod{26}$
$12 \equiv b \pmod{26}$

Jadi, b = 12

Persaman enkripsi: $C \equiv mP + b \pmod{n} \rightarrow C \equiv 195P + 12 \pmod{26}$

Dekripsi: $P \equiv m^{-1}(C - b) \pmod{n} \rightarrow m^{-1} = ??$

$19^{-1} \pmod{26} = 11$

Jadi, persamaan dekripsi: $P \equiv 11(C - 12) \pmod{26}$

Cipherteks IZW dikodekan menjadi 8, 25, 22

C = 8 $\rightarrow P \equiv 11(8 - 12) \pmod{26} = 8 \rightarrow$ huruf I

C = 25 $\rightarrow P \equiv 11(25 - 12) \pmod{26} = 13 \rightarrow$ huruf N

C = 22 $\rightarrow P \equiv 11(22 - 13) \pmod{26} = 6 \rightarrow$ huruf G

Jadi, plainteks dari NAG adalah ING (salah satu trigram yang sering muncul di dalam Bahasa Inggris)

6. **(Nilai = 5 + 5)** (a) Apa hasil operasi berikut dalam heksadesimal: 4BC91F ⊕ BA1DEC?
(b) Apa hasil perkalian F2 · B9 dalam $GF(2^8)$. Polinom irreduced polynom yang digunakan adalah $x^8 + x^4 + x^3 + 1$

Jawaban:

(a)

```
4BC91F = 0100 1011 1100 1001 0001 1111
BA1DEC = 1011 1010 0001 1101 1110 1100
------------------------------------ ⊕
         1111 0001 1101 0100 1111 0011
   F  1   D 4  F   3
```

(b)

F2 = 11110010 ⇒ $f(x) = x^7 + x^6 + x^5 + x^4 + x$

B9 = 10111001 ⇒ $g(x) = x^7 + x^5 + x^4 + x^3 + 1.$

F(x)g(x) = $(x^7 + x^6 + x^5 + x^4 + x)(x^7 + x^5 + x^4 + x^3 + 1) =$

$x^{14} + x^{13} + 2x^{12} + 3x^{11} + 3x^{10} + 3x^9 + 3x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + x$ (mod 2 setiap koefisien)
$= x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x$ (mod $x^8 + x^4 + x^3 + 1$) = $x^7 + x^4 + x^3$ = 10011000 = 98

7. **(Nilai = 15)** Sebuah plainteks (dalam heksadesimal), 4F51AC dienkripsi dengan sebuah block cipher. Ukuran blok yang dienkripsi adalah 8-bit dan kunci yang digunakan adalah 8-bit, yaitu B4. Fungsi enkripsi E yang digunakan adalah sebagai berikut:
   (i) Geser bit-bit di dalam pesan sejauh 2 bit ke kanan secara siklik
   (ii) XOR-kan hasil langkah (i) dengan kunci

   Tuliskan hasil enkripsi (dalam heksadesimal) untuk plainteks tersebut jika block cipher dioperasikan dengan mode:
   (a) ECB
   (b) CBC, IV = 00001111
   (c) Counter, dimulai dari counter awal 00000000

Jawaban:

(a) ECB: **67E09F**

(b) CBC: **A4C9ED**

(c) Counter: **FBA598**

Mode (a) ECB: Setiap blok dienkripsi **terpisah**, tanpa kaitan dengan blok lain.
Kunci K = B4 = 10110100

Blok 1

P_1 = 4F = 01001111_2
Geser 2 bit ke kanan = 11010011_2
XOR hasil pergeseran di atas dengan kunci K → C_1 = 11010011 ⊕ 10110100 = **01100111_2 = 67 (hex)**

Blok 2

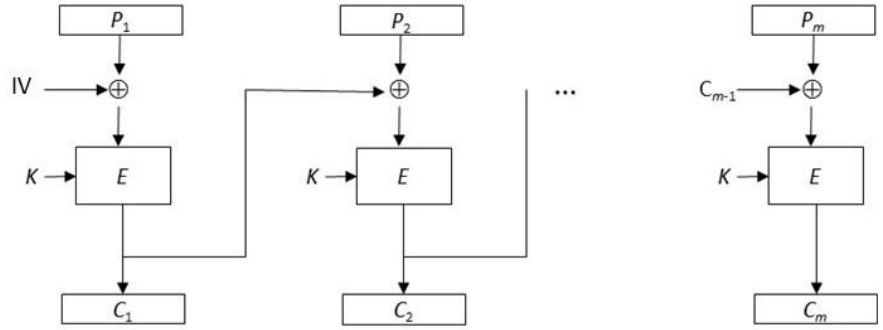
P_2 = 51 = 01010001_2
Geser 2 bit ke kanan = 01010100_2
XOR hasil pergeseran di atas dengan kunci K → 01010100 ⊕ 10110100 = **11100000_2 = E0 (hex)**

Blok 3

P_3 = AC = 10101100_2
Geser 2 bit ke kanan = 00101011_2
XOR hasil pergeseran di atas dengan kunci K → 00101011 ⊕ 10110100 = **10011111_2 = 9F (hex)**

Ciphertext (ECB) = 67E09F

Mode (b) CBC, IV = 00001111_2: $C_i = E(P_i \oplus C_{i-1}), C_0 = IV$
Kunci K = B4 = 10110100



Blok 1

P_1 = 01001111
IV = 00001111
XOR P_1 dengan IV = 01000000
Geser hasil di atas 2 bit ke kanan = 00010000
XOR hasil pergeseran di atas dengan kunci K = 00010000 ⊕ 10110100 = **10100100 = A4 (hex)**

Blok 2

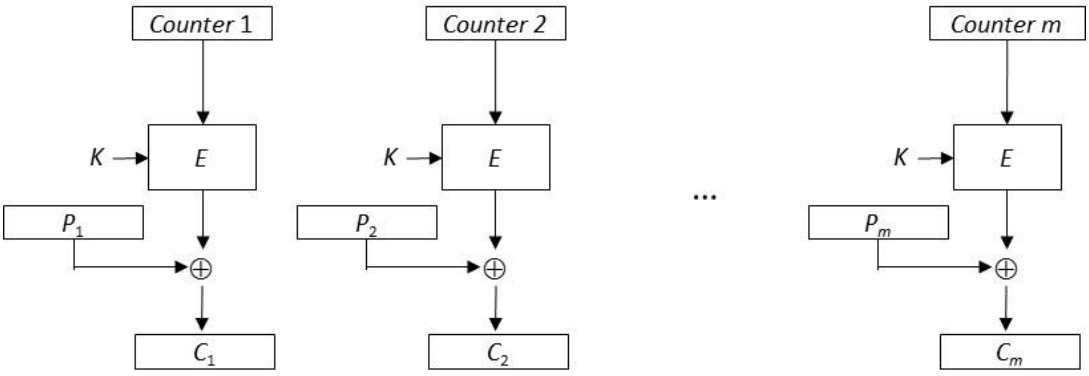
P_2 = 01010001
C_1 = 10100100
XOR P_2 dengan C_1 = 11110101
Geser hasil di atas 2 bit ke kanan = 01111101
XOR hasil pergeseran di atas dengan kunci K = 01111101 ⊕ 10110100 = **11001001 = C9 (hex)**

Blok 3

P_3 = 10101100
C_2 = 11001001
XOR P_3 dengan C_2 = 01100101
Geser hasil di atas 2 bit ke kanan = 01011001
XOR hasil pergeseran di atas dengan kunci K = 01011001 ⊕ 10110100 = **11101101 = ED (hex)**

Ciphertext (CBC) = A4 C9 ED

Mode (c) CTR, counter awal = 00000000_2: $C_i = P_i \oplus E(\text{Counter} + i)$



Counter 0: 00000000

Enkripsi counter:
Geser counter 2 bit ke kanan = 00000000
XOR hasil pergesaran dengan kunci K : 000000000 ⊕ 10110100 = 10110100 → $keystream_1$ = 10110100

P_1 = 01001111
XOR P_1 dengan $keystream_1$ → C_1 = 01001111 ⊕ 10110100 = **11111011 = FB (hex)**

Counter 1: 00000001

Enkripsi counter:
Geser counter 2 bit ke kanan = 01000000
XOR hasil pergesaran dengan kunci K : 01000000 ⊕ 10110100 = 11110100 → $keystream_2$ = 11110100

P_2 = 01010001
XOR P_2 dengan $keystream_2$ → C_2 = 01010001 ⊕ 11110100 = **10100101 = A5 (hex)**

Counter 2: 00000010

Enkripsi counter:
Geser counter 2 bit ke kanan = 10000000
XOR hasil pergesaran dengan kunci K: 10000000 ⊕ 10110100 = 00110100 → $keystream_3$ = 00110100

P_3 = 10101100
XOR P_3 dengan $keystream_3$ → C_3 = 10101100 ⊕ 00110100 = **10011000 = 98 (hex)**

Ciphertext (CTR) = FB A5 98

8. **(Nilai = 10)** Diketahui pasangan kunci publik dan kunci privat kepunyaan Tammy, Sonia, Farhan, dan Monalisa sebagai berikut:

Tammy:	**Sonia:**
Kunci public: (e, n) = (29,851)	Kunci public: (e, n) = (31,779)
Kunci privat: (d, n) = (1229,851)	Kunci privat: (d, n) = (1231,779)
Farhan:	**Monalisa:**
Kunci public: (e, n) = (41,899)	Kunci public: (e, n) = (121,1591)
Kunci privat: (d, n) = (881,899)	Kunci privat: (d, n) = (1537,1591)

Tammy mengirim pesan dan kunci enkripsi pesan (enkripsi menggunakan Vigenere Cipher) kepada Monalisa hybrid *cryptography* (RSA dan Vigenere Cipher). Pesan yang dienkripsi adalah SALAMSAYANGKUPADAMU dan kunci enkripsi adalah KOPIPAHIT. Cipherteks pesan dan cipherteks kunci dikirim bersamaan kepada Monalisa.
(a) Tuliskan cipherteks kunci dan cipherteks pesan yang dikirim oleh Tammy kepada Monalisa.
(b) Tuliskan hasil perhitungan dekripsi kunci dan dekripsi cipherteks yang diterima oleh Monalisa

Jawaban:
Tammy mengenkripsi kunci Vigenere dengan menggunakan kunci public Monalisa(e, n) = (121,1591):
Kunci = KOPIPAHIT = 10, 14, 15, 8, 15, 0, 7, 8, 19

A = 0, B = 1, C = 2, D = 3, E = 4, F = 5, G = 6, H = 7, I = 8, J = 9, K = 10, L = 11, M = 12, N = 13, O = 14, P = 15
Q = 16, R = 17, S = 18, T = 19, U = 20, V = 21, W = 22, X = 23, Y = 24, Z = 25

Enkripsi RSA: $c = p^e \bmod n$
$p = 10 \rightarrow c = 10^{121} \bmod 1591 = 676$
$p = 14 \rightarrow c = 14^{121} \bmod 1591 = 273$
$p = 15 \rightarrow c = 15^{121} \bmod 1591 = 834$
$p = 8 \rightarrow c = 8^{121} \bmod 1591 = 452$
$p = 15 \rightarrow c = 15^{121} \bmod 1591 = 834$
$p = 0 \rightarrow c = 0^{121} \bmod 1591 = 0$
$p = 7 \rightarrow c = 7^{121} \bmod 1591 = 1254$
$p = 8 \rightarrow c = 8^{121} \bmod 1591 = 452$
$p = 19 \rightarrow c = 19^{121} \bmod 1591 = 893$
Hasil enkripsi kunci: 676, 273, 834, 452, 834, 0, 1254, 452, 893

Enkripsi SALAMSAYANGKUPADAMU dengan Vigenere Cipher, hasilnya cipherteks: COAIBSHGTXUZCEAKIFE

Tammy mengirim {676, 273, 834, 452, 834, 0, 1254, 452, 893} dan COAIBSHGTXUZCEAKIFE kepada Monalisa

Monalisa mula-mula mendekripsi cipherteks kunci dengan menggunakan kunci privatnya (1537,1591)

Dekripsi RSA: $p = c^d \bmod n$
c = 676 → p = $676^{1537} \bmod 1591 = 10$
c = 273 → p = $273^{1537} \bmod 1591 = 14$
c = 834 → p = $834^{1537} \bmod 1591 = 15$
c = 452 → p = $452^{1537} \bmod 1591 = 8$
c = 834 → p = $834^{1537} \bmod 1591 = 15$
c = 0 → p = $0^{1537} \bmod 1591 = 0$
c = 1254 → p = $1254^{1537} \bmod 1591 = 7$
c = 452 → p = $452^{1537} \bmod 1591 = 8$
c = 893 → p = $893^{1537} \bmod 1591 = 19$
Hasil dekripsi kunci: 10, 14, 15, 8, 15, 0, 7, 8, 19 = KOPIPAHIT

Monalisa mendekripsi cipherteks pesan COAIBSHGTXUZCEAKIFE dengan kunci KOPIPAHIT, hasilnya plainteks SALAMSAYANGKUPADAMU

9. **(Nilai = 10)** Diketahui kunci publik RSA Alice adalah (e, n) = (7, 187). Misalkan Eva memperoleh 3 buah cipherteks yang dikirim oleh Bob kepada Alice adalah 145, 108, 93. Eva mendekripsi ketiga buah cipherteks tersebut, lalu men-*decode* nya menjadi huruf-huruf plainteks (A = 0, B = 1, C = 2, …, Z = 25). Tuliskan plainteks yang didekripsi oleh Eva.

Jawaban:

1. Faktorkan $n = 187 = 11 \times 17$.
   $\varnothing(n) = (11-1)(17-1) = 10 \cdot 16 = 160$.
2. Cari d sehingga $7d \equiv 1 (\mathrm{mod}\ 160)$. Diperoleh $d = 23$ karena $7 \cdot 23 = 161 \equiv 1 (\mathrm{mod} 160)$.
3. Dekripsi tiap ciphertext $c$dengan $m \equiv c^d (\mathrm{mod} 187)$:

   - $m_1 = 145^{23}\, mod\, 187 = 19$
   - $m_2 = 108^{23}\, mod\, 187 = 14$
   - $m_3 = 93^{23}\, mod\, 187 = 15$

4. Konversi angka ke huruf (A=0, B=1, …, Z=25):

   - $19 \rightarrow T$
   - $14 \rightarrow O$
   - $15 \rightarrow P$

Jadi plainteks yang didekripsi Eva adalah **"TOP"**.

10. **(Nilai = 10)** Alice dan Bob akan berbagi kunci enkripsi simetri yang sama menggunakan algoritma Diffie-Hellman. Alice dan Bob menyepakati g = 10 dan p = 71. Alice memilih kunci privatnya a = 10 dan Bob memilih kunci privatnya b = 12. Tinjau dua kasus:
    (a) Kasus 1: tidak terjadi *man-in-the-middle attack*. Tentukan kunci enkripsi simetri yang dihasilkan oleh Alice dan Bob
    (b) Kasus 2: terjadi *man-in-the-middle attack*. Tiba-tiba Mallory mengintersepsi komunikasi dan melakukan serangan *man-in-the-middle attack* untuk mengetahui kunci enkripsi simetri Alice (K1) dan kunci enkripsi simetri Bob (K2). Mallory menggunakan kunci privatnya m = 15 di dalam serangan itu. Tentukan kunci enkripsi K1 dan K2 yang diperoleh oleh Mallory.

Jawaban:
(a)
Kunci public Alice: $A = 10^{10} \bmod 71 = 30$

Kunci public Bob: B = 10^{12} mod 71 = 18

Alice mengirim A = 30 kepada Bob
Bob mengirim B = 18 kepada Alice

Alice menghitung: K = 18^{10} mod 71 = 37
Bob menghitung: K = 30^{12} mod 71 = 37

Jadi, kunci simetri bersama Alice dan Bob adalah 37

(b)

Mallory menggantikan nilai publik yang dikirim oleh Alice dan Bob:
Mallory menghitung $M = g^m \, mod \, p = 10^{15} \, mod \, 71 = 37.$

Proses intersepsi:

- Alice menerima M(mengira itu Bob) dan menghitung kunci dengan Mallory:
$$K_1 = M^a \, mod \, p = 37^{10} \, mod \, 71 = 30.$$
- Bob menerima M(mengira itu Alice) dan menghitung key dengan Mallory:
$$K_2 = M^b \, mod \, p = 37^{12} \, mod \, 71 = 32.$$

Mallory dapat menghitung kedua kunci juga karena ia tahu m:

- Dengan A yang ditangkap, Mallory dapat menghitung $K_1 = A^m \, mod \, p$ = 30^{15} mod 71 = 30
- Dengan B yang ditangkap, Mallory dapat menghitung $K_2 = B^m \, mod \, p$ = 18^{15} mod 71 = 32

Jadi hasil serangan:

- Kunci antara Alice dan Mallory (mengira itu Bob): K_1 = 30
- Kunci antara Bob dan Mallory (mengira itu Alice): K_2 = 32

LAMPIRAN Vigenere Square

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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