March 20th, 2017

German University in Cairo
Media Engineering and Technology
Lecturer: Amr El Mougy
TA: Alaa Gohar and Heba Anwar

Computer and Network Security

Spring term 2017
Midterm Exam

Bar Code

Instructions: Read carefully before proceeding.

CSEN	DMET

1) Duration of the exam: 2 hours (120 minutes).
2) (Non-programmable) Calculators are allowed.
3) No books or other aids are permitted for this test.
4) This exam booklet contains 11 pages, including this one. **Note that if one or more pages are missing, you will lose their points. Thus, you must check that your exam booklet is complete.**
5) Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem or on the extra sheets and make an arrow indicating that.
6) When you are told that time is up, stop working on the test.
7) Include any assumptions that you need to make.
8) Follow the instructions of your proctors under all circumstances.

Good Luck!

Don't write anything below ;-)

Exercise	1	2	3	4	5	Σ
Marks	10	15	20	20	20	85
Final Marks						

Question 1:

Specify if the following statements are True (T) or False (F). If you need to justify your answer, please do so in the space provided.

1) An attacker changing the contents of a message on its way from the sender to the receiver is an example of a passive attack.	F
2) In public key cryptography, encrypting a message with the private key of the sender ensures confidentiality of the message.	F
3) The Vigenere cipher is not vulnerable to frequency analysis attacks.	F
4) Link encryption means that the contents of a packet as well as its headers will be encrypted.	T
5) The electronic codebook (ECB) mode of encryption can be safely used to exchange one-time messages.	T
6) A security certificate binds the public key of a user to his/her identity.	T
7) AES is considered an implementation of the Feistel cipher.	F
8) Traffic analysis, where an attacker examines the patterns of communication between a sender and a receiver is an example of a passive attack.	T
9) The output feedback (OFB) mode of encryption uses a nonce instead of an initial value (IV) to encrypt the first block.	T
10) Any cipher that uses a key that has the same length as the message to be encrypted is considered a one-time pad.	F

Extra space for justification:

Question 2:

The following ciphertext was encrypted with the Vigenere cipher:

I	**V**	**I**	**V**	**Y**	**G**	**A**	**R**	**M**	**L**	**W**	**Y**	**I**	**V**	**I**	**K**	**F**	**D**	**I**	**V**	**I**	**F**	**R**	**L**

a) What is the most likely length of the key?
b) If the first two letters of the key are "PO", and the last two letters of the key are "RY", deduce the key and decrypt to obtain the plaintext.

Answer 2:

a) The letters "I V I" are repeated three times. The distance between the first and second occurrence is 12, and the distance between second and third occurrence is 6. Thus, the most likely length of the key is gcd(6, 12) = 6.

b) Since the most likely length of the key is 6, then divide the letters into 6 columns

I	V	I	V	Y	G
A	R	M	L	W	Y
I	V	I	K	F	D
I	V	I	F	R	L

Looking at the third column, we can guess that I corresponds to the plaintext letter E, since it the most frequently occurring letter, which means that the key letter is also E. In addition, the first two and last two letters are given. Thus, the only remaining letter of the key is the fourth one. At this step, we can decrypt the given letters to get some insight

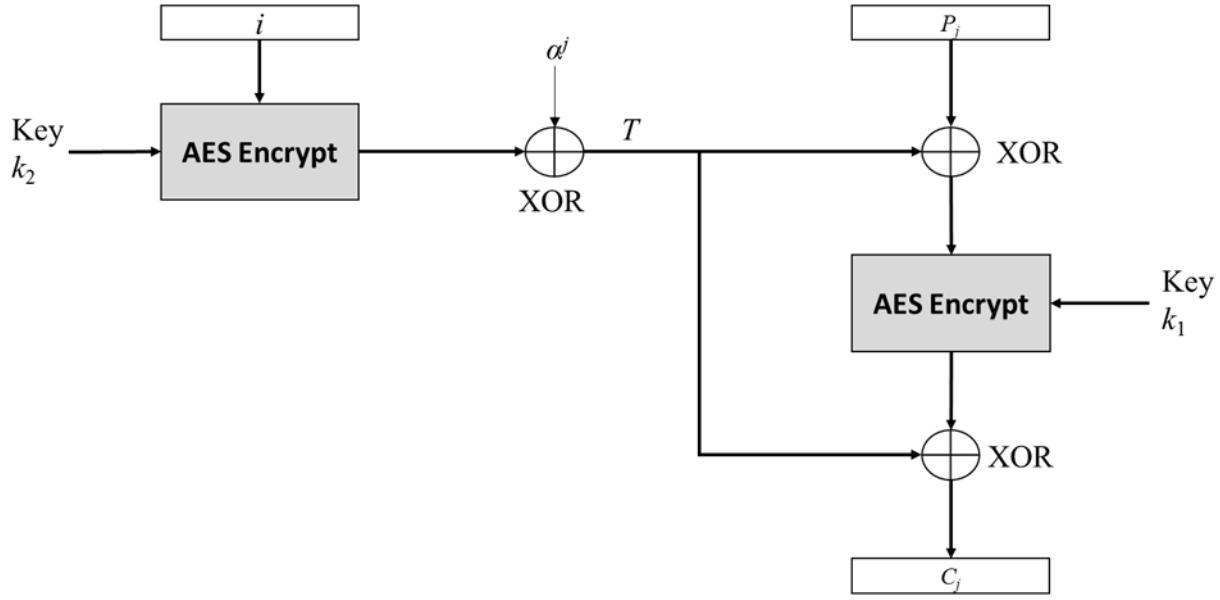
I	V	I	V	Y	G	A	R	M	L	W	Y	I	V	I	K	F	D	I	V	I	F	R	L
P	O	E		R	Y	P	O	E		R	Y	P	O	E		R	Y	P	O	E		R	Y
T	H	E		H	I	L	D	I		F	A	T	H	E		O	F	T	H	E		A	N

Now it is easy to guess that the remaining letter of the key is T. An alternative to guessing is to brute force the remaining letter until a meaningful phrase is obtained. Thus, adding the remaining letter, we get

I	V	I	V	Y	G	A	R	M	L	W	Y	I	V	I	K	F	D	I	V	I	F	R	L
P	O	E	T	R	Y	P	O	E	T	R	Y	P	O	E	T	R	Y	P	O	E	T	R	Y
T	H	E	C	H	I	L	D	I	S	F	A	T	H	E	R	O	F	T	H	E	M	A	N

Question 3:

The figure below shows the encryption diagram for the AES-XTS mode of encryption, which is used for data storage. In the figure, i, is a 128-bit value known as the tweak that is rarely changed, j is the number of the disk sector to be encrypted, α is a 128-bit fixed value, P_j is the data block in the j^{th} sector to be encrypted, and C_j is the resulting ciphertext. The system uses two symmetric keys k_1 and k_2 for the AES blocks.



a) Determine the formula for encryption (for calculating C_j).

b) Determine the formula for decryption and draw the decryption algorithm.

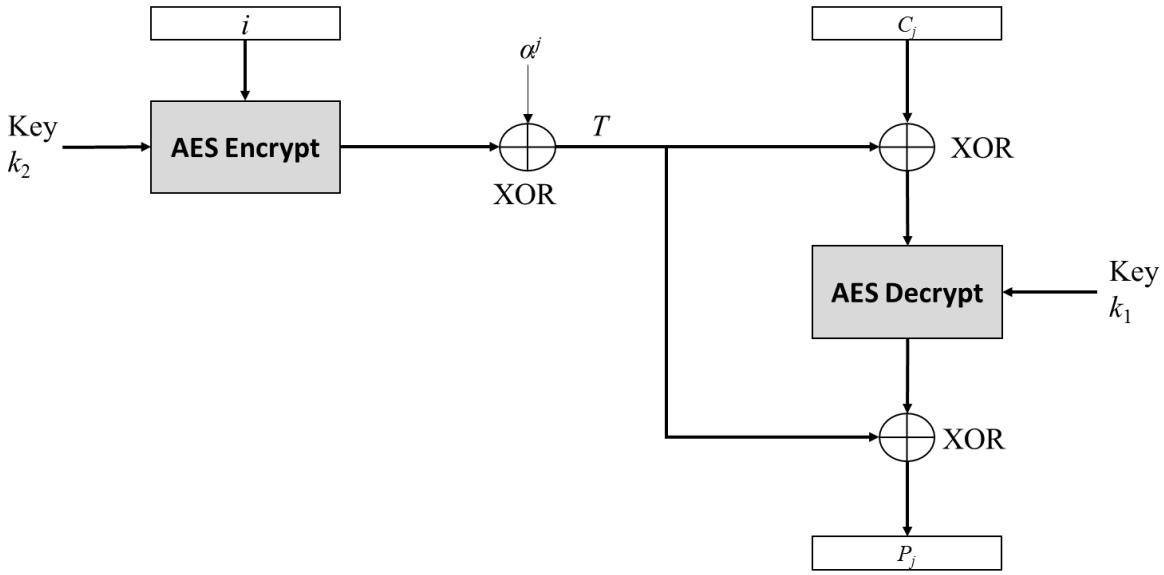
c) If an error occurs in the j^{th} block of ciphertext (C_j), how many blocks will be affected in the decryption?

Answer:

a) $T_j = E_{K2}(i)$ XOR α^j

$C_j = E_{K1}(P_j$ XOR $T_j)$ XOR T_j

b)



$T_j = E_{K2}(i)$ XOR α^j

$P_j = E_{K1}(C_j$ XOR $T_j)$ XOR T_j

c) There is no chaining, errors do not propagate.

Question 4:

The figure below shows the S-box and inverse S-Box used in encryption and decryption of AES.

(a) S-box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(b) Inverse S-box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

a) Encrypt the following block

05	AA	43	45
F1	BC	31	88
71	C6	7E	12
54	AB	5C	D3

b) Using the encrypted block, show that the S-Box is not self-inverting (simply show one example).

c) Using the encrypted block, show that the S-Box has no fixed points (simply show one example).

Answer:

a) Encrypted block:

6B	AC	1A	6E
A1	65	C7	C4
A3	B4	F3	C9
20	62	4A	66

b) Take any block, for example S-Box(AA) = AC, but IS-Box(AA) = 62, thus it is not self-inverting.

c) For example S-Box(F1) = A1, but A1 is not equal to F1.

Question 5:

a) Can a user in an RSA system choose a value for the public key exponent, *e*, to be even? (*e.g.* $e = 4$). Justify your answer.

b) In a particular RSA system, Alice has a public key {15, 391}, while Bob has public key {11, 319}. Alice needs to send a message $M = 5$ to Bob that is digitally signed and confidential. Calculate the value of the ciphertext *C* after Alice performs the two-step encryption process.

Answer:

a) No, since *p* and *q* are prime numbers, then they are always odd numbers. Thus, $\phi(n) = (p - 1)(q - 1)$ is always an even number. This means that the gcd(e, ϕ(n)) cannot be equal to 1 if *e* is even.

b) First Alice has to encrypt with her private key to perform the digital signature, then encrypt with Bob's public key.

To obtain Alice's private key, we factorize 391 into 17 and 23. Thus, $\phi(n) = 352$.

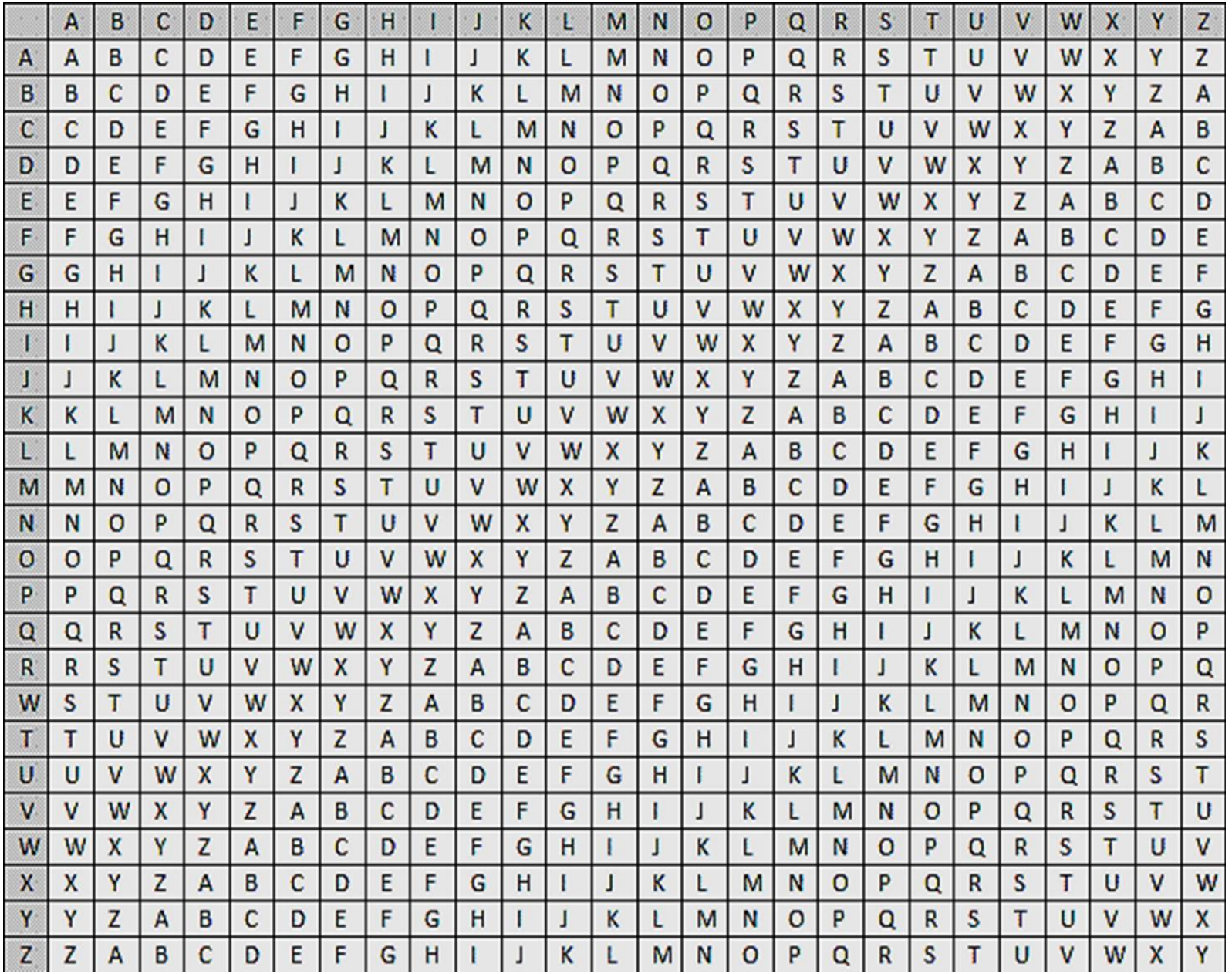
Now we solve $15x + 352y = 1$

We get $352 - 23(15) = 7$

And $15 - 2(7) = 1$ → substituting we get $15 - 2(352 - 23(15)) = 1$ → which can be rearranged to $15(47) - 2(352) = 1$. Thus, $d = 47$

Now we can encrypt to $5^{47} \bmod 391 = [(5^{13} \bmod 391)(5^{13} \bmod 391)(5^{13} \bmod 391)(5^{8} \bmod 391)] \bmod 391 = [343*343*343*16] \bmod 391 = 194$

Now we can encrypt using Bob's public key $194^{11} \bmod 319 = [(194^{4} \bmod 319)\ (194^{4} \bmod 319)\ (194^{3} \bmod 319)] \bmod 319 = [36*36*112] \bmod 319 = 7$



	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
W	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