Solutions: Sheet 3

1. Kerckhoff ’s Principle

Name the three main properties that Auguste Kerckhoffs specified as requirements for a cryptosystem.

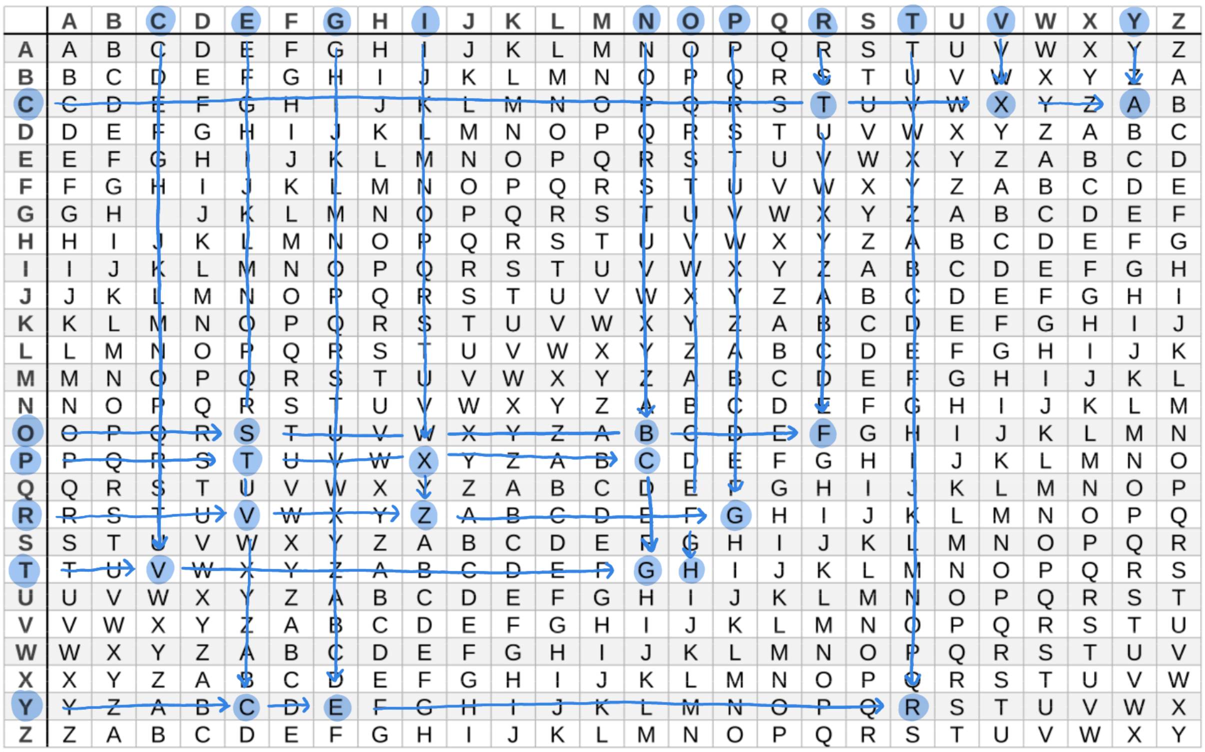
- If a system is not provably secure, it should be practically secure.
- The design of a system should not require secrecy and should not be a problem if it falls in the hands of the enemy.
- A cryptosystem must be easy to use.

2. Vigenere Encryption

The plaintext is `VIGENEREENCRYPTION`, the keyword `CRYPTO`. What is the Vigenere encrypted ciphertext?

Document the derivation of the ciphertext in a comprehensible manner.

```
Ciphertext VIGENEREENCRYPTION
       Key CRYPTOCRYPTOCRYPTO
 Plaintext XZETGSTVCCVFAGRXHB
```



	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

3. Vigenere Encryption (II)

Crack the following Vigen`ere encrypted ciphertext. What is the key?

```
TKETOXSQSWOADRNMSOISHWRUSHJGSWOZTKEQDJEAFWHQVLLXAJEUTVTAOGOZIWSAWQAZDO
OAKHDAUWOHEUANRRAPSSRQAGORWHSFCRUZTUYRAUMXAQDZOWADEPADKDBXEKOGSHBKAQYY
```

```
EDNEIWWMSDBAUWTTIUTKYHADSRLPSTUMTWIEHVQGAUIEHPAPERFNRLCWAQDTAGFAUUWUNG
OISVEFIQTTEIRANWORAVILEDNPPUOBOUTUOQWTIFHYOUEAROEESHXMCWLKFDIXEGTAPOEM
SHTTEHYQTKEANOYBEUSANIODWKOYTKETOXSQWDSUNDNKWDYEPHCUAOWMSDRFHXRPEQTMNG
TTAWWMSRNXYEEOAXSQIWHMPSEZEGTABHTTERNQHHLUVHDUNKETAGLUVHDUNLTROUANOXTF
HUEQYHADSHVQRVIZCHHQHDDYOYEPOXTAFOOZDRNNEFAGSHIFMDDQHLMZEUVAUVAZDLRDIW
ANLHHQWDSMBRUFTKIDTBAEWHLXTDLXDDRWHDIDEGAZDQEHEUQGIWEMTHAEEZIFHKIYSHLR
TKEFHLNSTKAFUVEPTRWARUYTIPMASWWMSWHQFDCFTKAFPHOBLHAXWDYEUVEPTRAEKKIYWK
AFHHWMSOOAKLNSSRWARUIQDDBAUWHQWRRWEGIZLRCMLUAPIRWTIFHTEDLIABSGSHDFOWEX
LKIEFUIQNGSIAVAXOWMARHIZTHRQSWIZGWHMNWHQYSRABDBXYWHAUJHFIWWMSWOAMRSFOI
HUSIRUEQDEWRRWEGIZAGVQRWIEIQG
```

```
Key = ADAM
```

```
THE HOUSE STOOD ON A SLIGHT RISE JUST ON THE EDGE OF THE VILLAGE IT STOOD ON
ITS OWN AND LOOKED OUT OVER ABROAD SPREAD OF WEST COUNTRY FARMLAND NOT ARE
MARKABLE HOUSE BY ANY MEANS IT WAS ABOUT THIRTY YEAR SOLD SQUATTISH SQUARISH
MADE OF BRICK AND HAD FOUR WINDOWS SET IN THE FRONT OF A SIZE AND PROPORTION
WHICH MORE OR LESS EXACTLY FAILED TO PLEASE THE EYE THE ONLY PERSON FOR WHOM
THE HOUSE WAS IN ANYWAY SPECIAL WAS ARTHUR DENT AND THAT WAS ONLY BECAUSE IT
HAPPENED TO BE THE ONE HELIVED IN HE HAD LIVED IN IT FOR ABOUT THREE YEARS
EVER SINCE HE HAD MOVED OUT OF LONDON BECAUSE IT MADE HIM NERVOUS AND
IRRITABLE HE WAS A
```

4. Brute Force Attack

(a) Explain the term brute force attack and its chances of success in the context of encryption.

A brute force attack is one in which as many possibilities are tried in hopes of guessing correctly in the end. An crypto method is considered practical secure if there are $2^{\geq 100}$ keys and the attacker has unlimited resources.

(b) What percentage of all possible binary keys with key length 128 bits can be tried in 1.000.000 years if 10.000.000 keys can be tested per second?

$$\frac{10.000.000 \times 24 \times 30 \times 365 \times 1.000.000}{2^{128}}$$

5. One-Time Pad

Encrypt the message `Crypto` comprehensibly using the one-time pad encryption technique. Use the 6-digit string `000000` as key (one-time pad). Use ASCII as bit representation for the message and the key.

```
Plaintext    C        r        y        p        t        o
     Bits 01000011 01110010 01111001 01110000 01110100 01101111
                              XOR
      Key 00110000 00110000 00110000 00110000 00110000 00110000
```

```
                                             =
  Message 01110011 01000010 01001001 01000000 01000100 01011111
```

6. One-Time Pad Security Level

Explain why a message encrypted by this method cannot be recovered without knowing the used encryption key. What level of security (number of possible keys) does the one-time pad encryption provide in the previous question, if it is known that a 6-ASCII-character combination has been selected as the key? Write down your solution and use the 2^n notation for your solution.