JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Fachbereich Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security

Fachbereich

Institut für Wirtschaftsinformatik
Lehrstuhl für M-Business & Multilateral Security
www.m-chair.de

Prof. Dr. Kai Rannenberg
Sascha Löbner, MSc.

E-Mail security@m-chair.de

Information and Communications Security SS 2022 Assignment 3 *Cryptography*

Please prepare your solutions for the following exercises. We will discuss them on the 21st of June 2022.

Exercise 1 (Caesar Cipher)

A Caesar encryption is given by the following encryption function:

$$e_k: \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}, \qquad x \rightarrow (x + k) \quad mod\ 26$$

with $k \in \mathbb{Z}_{26}$

a) Encrypt the message "perfect indistinguishability" using e_{10}.

b) What is perfect indistinguishability?

c) Does the condition of perfect indistinguishability hold in general for the Caesar Cipher? Give a two-line explanation.

d) What attacks can be used to break the Caesar Cipher?

Exercise 2 (Stream Ciphers)

a) What is a one-time pad (Vernam-code)?

b) Zoe wants to encrypt the letter Z. The letter is given in ASCII code. The ASCII value for Z is $90_{10} = 1111010_2$. Using Vernam-code, which of the following keys are suitable to encrypt this plaintext?

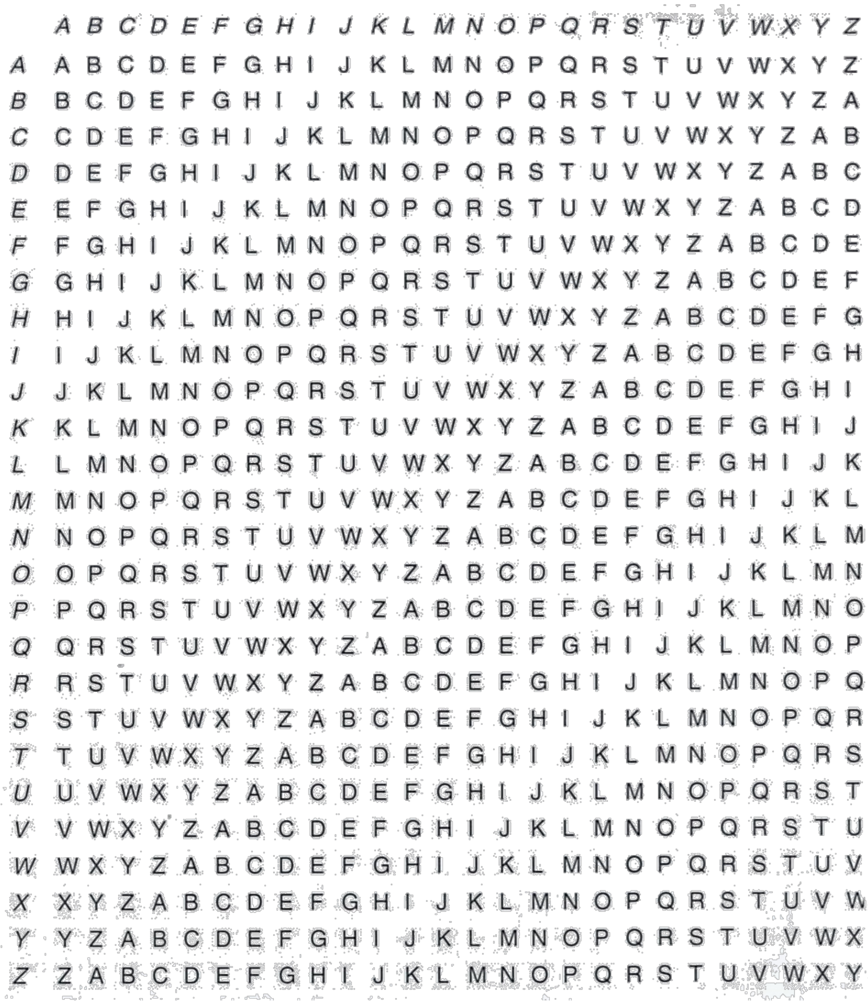
b1) 11100100
b2) 0011101
b3) 101011

c) Encrypt the message using Vernam-code, XOR as an encryption function and the key in b).

Exercise 3 (Vigenère Cipher)

a) What is the Vigenère Cipher?

b) In the following you are given the key $k = "GOETHE"$ and the cyphertext $c =$ "CSWMLRJWWMOISCWMIIGIXBMYRQEFWYY". Identify the message m using the running key variant as given in the lecture. Show the necessary steps (use the Vigenére tableau below when necessary).

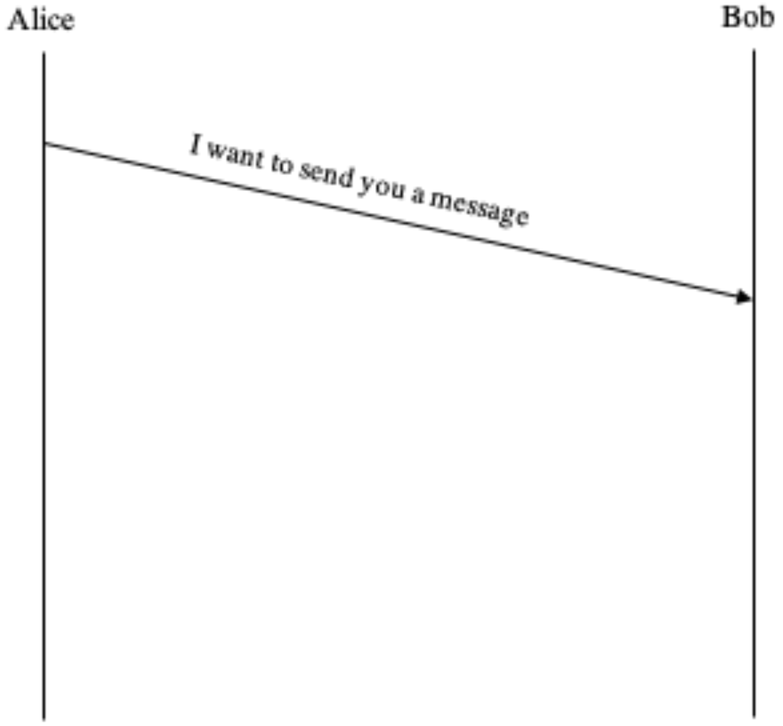


	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U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

Exercise 4 (Asymmetric Cryptosystems and RSA)

a) Describe differences between symmetric and asymmetric cryptosystems.

b) Alice wants to send a message m to Bob. Because the message is a secret, Alice encrypts the message using RSA. Complete the flow chart below and also show the necessary calculation steps for encryption and decryption. Indicate which information are public or known only by Bob or Alice.



c) Consider an RSA cryptosystem. The following keys were made public: $e = 5, n = 21$.

i. Encrypt the message $m = 3$ using RSA
ii. Determine p and q (factorize n).
iii. Determine the private key d.
iv. Decrypt the cyphertext and check that the result is $m = 3$
v. What is the problem with the chosen keys?

d) Decrypt the message c = 2 using RSA. The private key of the receiver is $d = 3$ and $n = 15$.

e) Let $n = 221$. Use Fermat's factorization to factorize n. (Hint: $n = x^2 - y^2 = (x + y)(x - y)$)

f) Why is it possible to break RSA with Post-Quantum Cryptography?