INF2005 Cyber Security Fundamentals

Cryptography Lab (Week 1)

CRYPTOGRAPHY EXERCISES

1. In cryptography, plain text is encrypted to cipher text and sent. Anybody intercepting the message would encounter some difficulty trying to read or recover the original plain text.

   Browse to: https://www.online-toolz.com/tools/text-encryption-decryption.php

   Experiment with encrypting and decrypting several messages. How does a receiver read or recover the plain text?

2. Browse to the site: https://www.kerryveenstra.com/cryptosystem.html

   Experiment with encrypting and decrypting using different shared secret keys.

   This is symmetric key cryptography in which both sender and receiver shares the same secret key.

3. Browse to: https://www.devglan.com/online-tools/rsa-encryption-decryption

   Experiment with different public and private key pairs (select Cipher Type as RSA).

   Then, use either key to encrypt / decrypt and the corresponding paired key to decrypt / encrypt.

   Can you use the same key to encrypt as well as decrypt?

   What have you learnt from this experiment?

4. Browse to the blowfish site: https://encode-decode.com/blowfish-encrypt-online/

   The key is SIT-UOG. Try to decrypt the following message:

   X9NZsUj2CY3XkuJQyqfQYDErvHfLN2I+QNt5qZyab2a2++eH5+wMkAzEjiwY4RKdusMb
   WAKRYGN+Qv8wLm4t+9EFCYR8dZjpdDSUeUTJZmY=

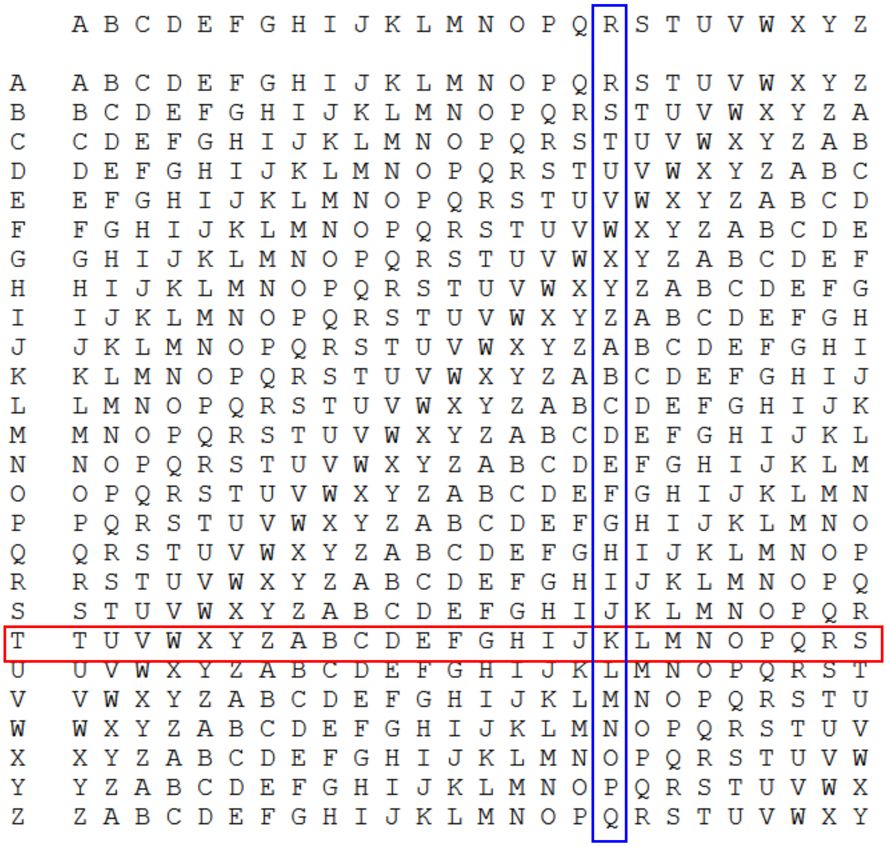
5. Asymmetric key cryptography can also be used for authentication of sender. Browse to: https://www.kerryveenstra.com/cryptosystem.html again.

   When a receiver with the public key of a key pair decrypts a received cipher text, what can be inferred here? Is authentication the same as confidentiality?

6. What is the main weakness in both symmetric and asymmetric key cryptography seen in the above? Is there a way to overcome this weakness? Browse to the site: https://www.dcode.fr/diffie-hellman-key-exchange

7. A simple substitution cipher is Caser Cipher. Browse to the following site: https://cryptii.com/pipes/caesar-cipher. What happens when the shift distances exceed ±26?

8. Vigenere Cipher is a polyalphabetic substitution cipher based on the following key table:



	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

The keyword is RELATIONS. Decrypt the following cipher text:

`KS ME HZ BBL KS ME MPOG AJ XSE JCSFLZSY`

9. A Diffie-Hellman key exchange was used to generate a shared secret key for Alice and Bob. Assume known parameters to be: modulus p = 11, generator G = 2, Alice's private random number, a = 9, Bob's private number, b = 4. Compute **manually** the shared secret key.

10. Browse to the following site: https://cryptii.com/pipes/rail-fence-cipher

    Experiment with different rail key values to see the effects of rail fence cipher.

    https://www.boxentriq.com/code-breaking/rail-fence-cipher (ignore offset).

CRYPTANALYSIS CHALLENGES

[You may need to use online tools]

11. Break the following code:

```
UGRhIGx3b29za256IGJrbiBwZGEgeWR3aGhhamNhIGx3Y2EgZW86IHludWxwaw==
```

[Hint: there is a reason for '==' at the end]

12. The following is a columnar transposition cipher. Try to break it!

PRRO IEACLCHSEO (Hint: Key is KEY <-> YEK)

13. Decode the following:

- .... . .--. .- ... .-- --- .-. -.. ..-. --- .-. - ....-.. . ...- . .-.. .. ... .-- . .-.. .-.. -.. --- -. .

[Hint : military use, use online tool]

14. Write a simple Python program (or use online tools) to combine the binary bit **strings** here with **XOR** to get the password:

```
1001001100101001100101001000011010100101000101011010011101O
```

[Hint: XOR -> hex -> ascii]

15. Decode the following decimals to find the password:

```
8490910490910190911290997909115
909115909119909111909114909100
909105909115909100909101909999909999
909111909110909118909101909114909116
```

[Hint: at a glance, observe anything? see any pattern? What can it be?]

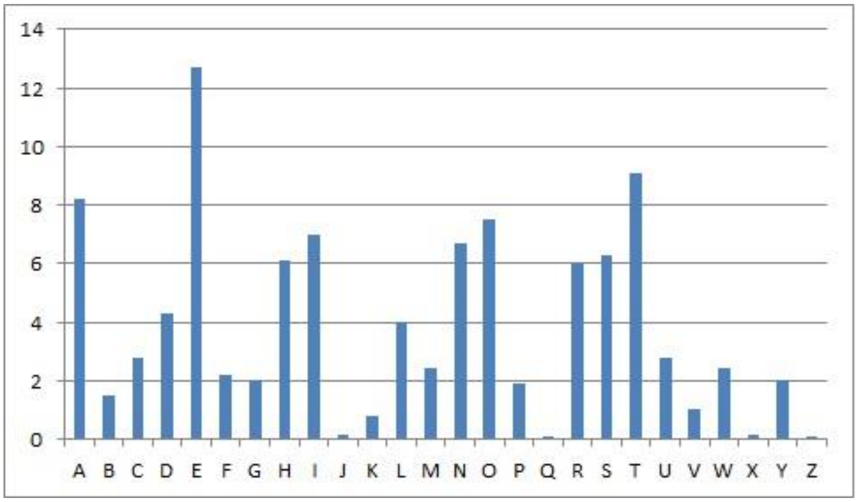
16. Decode the following phrase to find the password for this challenge:

```
8i4 q5tt/>/>1se g1s 8i4 di5mm4oa4 t284 2t; 4mju4
```

17. In this question, we shall use Frequency Analysis to break the code used to encrypt the intercepted ciphertext below, given that it has been encrypted with a Monoalphabetic Substitution cipher.

GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU', MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS

The Standard English Letter Frequencies are shown in the following histogram (H1):


14
12
10
8
6
4
2
0
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