Name: Stephen Lankford

OIT CSET

**CST 407 Prof. N.**

**TEST#1, SU20**

1. (2 Pts) In a typical non-propriety/commercial private–key cryptosystem, only the encryption algorithm and decryption algorithm MUST be kept secret at all time for the system to be safe. On the other hand, the encrypt and decrypt key need not be kept secret.
2. True
3. **False**
4. (2 Pts) Using a substitution-type cipher like Caesar, the number of occurrences of the character ‘a’ in plaintext must result in the same number of occurrences of the character ‘A’ in corresponding ciphertext.

(Note: for example, if “a” appears 10 times in plaintext, then “A” must appear 10 times in the corresponding ciphertext? Capital letters used in ciphertext is only a mean of differentiating. This question refers to the occurrence of the character ‘a’ in plaintext, ‘A’ in corresponding ciphertext. Linguistically, “a” or “A” is the same.)

1. True
2. **False**
3. (2 Pts) Using a transposition-type cipher like rail fence, the number of occurrences of the character ‘a’ in plaintext must result in the same number of occurrences of the character ‘A’ in corresponding ciphertext.

(Same note as in question#2 with the exception that it is a transposition cipher this time instead of substitution)

1. **True**
2. False
3. (2 Pts) Using the Caesar cipher using Phong’s CST407 class rules, all numbers must be spelled out. (i.e zero, one, one thousand…)
4. True
5. **False**
6. (2 Pts) When using Caesar cipher on any alphabet (English, French, Chinese, Arabic, Russian…) is simply a subset of the monoalphabetic ciphers, its key possibility is always only 26 out of the many keys of the monoalphabetic ciphers.
7. True
8. **False – not all alphabets use 26**
9. (2 Pts) In monoalphabetic ciphers, the number of keys is 2626
10. True
11. **False – 26!**
12. (2 Pts) Vignere is a poly-alphabetic system based on Caesar that depends on a repetitive pattern of keys in the encryption/decryption process.
13. **TRUE**
14. FALSE
15. (2 Pts) The best way to defeat any cipher systems is to use the brute force attack: decrypt using all the possible keys until a recovered message makes sense. No key system is safe enough with the limitless computing power that currently exists.
16. TRUE
17. **FALSE – i.e. brute force is not useful against AES128 because it would take an unreasonable number of years to crack with current technology**
18. (2 Pts) In the Vignere Tableau system, the keyword can have repeating letters

(for example, the keyword can be “hello” although “hello” has two l’s).

1. **TRUE**
2. FALSE
3. (2 Pts) Playfair is basically mono-alphabetic except Playfair is based on a 26 square table.
4. TRUE
5. **FALSE – 25 squares – I/J same square**
6. (5 Pts) Given the Caesar encryption equation

ciphertext = (plaintext + key) % 26

a. Provide the decryption equation for plaintext as a function of ciphertext:

**Plaintext = (Cipher – Key + 26) mod 26**

b. (5 Pts) For Caesar cryptosystem, if the integer value for ciphertext is 4 and the key is 21, what is the value of plaintext using your equation in part a) above

4 = E; 9 = J, 21 = V

**Plaintext = (4 – 21 + 26) mod 26 = 9**

1. (8 Pts) Using Playfair cipher and the key made up of the word “iwojimapacificocean”, provide the ciphertext for plaintext = te to fx fe ns iv eh ue ci ty

Show the completely filled-out Playfair square after the password is correctly placed.

**Answer: ciphertext = SN RA OR CF ET WU ME YP PW SZ**

i/j w o m a

p c f e n

b d g h k

l q r s t

u v x y z

1. (8 Pts) Use the same Playfair cipher with the same key “iwojimapacificocean”, decipher the following ciphertext: ZN TO OI/J CN SP UP

**Answer: plaintext = tarawapeleli**

1. ( 8 Pts) Using the polyalphabetic substitution cipher with the Modern Vignere tableau and the key of “airforceography”, cipher the following plaintext: rollingthunder

airforceography

rollingthunderr

**Answer: ciphertext = RWCQWEIXVAEDTYP**

1. (8 Pts) Using the polyalphabetic substitution cipher with the Modern Vignere tableau and the key of “mozart”, decipher the following ciphertext: T P L I F Z F K E B R R R R Q

mozartmozartmoz

t p l Ifzf kebrr r rq

**Answer: plaintext = hbmiogtwfbayfdr**

1. (8 Pts) Given a monoalphabetic cipher with key “alfredthayermahan” with no offset, encrypt the following plaintext: nelsonoftrafalgar

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 l f r e d t h y m n b c g I j k o p q s u v w x z

**Answer: ciphertext = gebpigidqoadabtao**

1. (8 Pts) Given a monoalphabetic cipher with key “greatesthits” with no offset, decrypt the following ciphertext: Q S O G E O C A R R I W

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

G r e a t s h I b c d f j k l m n o p q u v w x y z

**Answer: plaintext = tfracrjdbbhw**

1. (6 Pts) Using the 3-rotor machine with initial settings shown below, provide the top left side number of each of the three rotors after 555555 keystrokes. Here, we are assuming that each rotor clicks 26 times before it arrives back to its original position. Note the tops of the wheels rotate into the paper.

20 5 11

Slow Medium Fast (Rotors)

555555 % 26 = 13 555555 / 26 = 21367 21367 % 26 = 21 21367 / 26 = 821

821 % 26 = 15 821 / 26 = 31 31 % 26 = 5 31 / 26 = 1 1 % 26 = 1 1 / 26 = 0

555555 13

21367 21

821 15

31 5

1. 1

0

20 5 11

+ 1 5 15 21 13

**9 0 24**

1. (8 Pts) Using the Caesar cipher, key = 12:

Decrypt the ciphertext: T A D E Q E T A Q O D M N

**Answer: plaintext = H O R S E S H O E C R A B**

1. (8 Pts) Using the Phong’s CST407 rail fence technique of transposition, given a rail fence depth of 3, decipher the following ciphertext: HHHIMIONIEEETACUOTYYYSGYKWX

HHHIMIONI

EEETACUOT

YYYSGYKWX

Note: plaintext in this case will make sense

**Answer: plaintext = HEY HEY HEY ITS MAGIC YOU KNOW IT X**