Usman Institute of Technology

**Mid-Term Examination Fall 2020 Semester**

**Course Code:** CS413 **Course Title:** Information Security  **Date:** Jan 01, 2021

**Maximum Marks:** 30 **Max Time Allowed:** 1.5 hours for solving and uploading the paper.

**PLEASE FILL IN THE FOLLOWING BEFORE PROCEEDING**

**Seat No. ST-18045** **Roll No.** **18B-129-SE**

**Batch**: **2018**

# **Declaration**

I guarantee that all submissions are based on my independent work without any unauthorized help. All activities are completed with full adherence to the “Ethics Policy” of the Institute. I understand that any breach would result in disciplinary action against me as per Institute rules.

I **have read and understood the Students Ethics Policy for Online Assessments.**

**(paper will not be graded if the above is not checked)**

**Note:** Submission of this paper certifies that you are agreed to the Students Ethics Policy for Online Assessments and are liable to be judged according to it.

**AWARD**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | **Q1** | **Q2** | **Q3** | **Q4** | **Q5** | **Q6** | **Q7** | **Q8** | **Q9** |
| **Examiner** | |  |  |  |  |  |  |  |  |  |  |
| **ERC** | |  |  |  |  |  |  |  |  |  |  |
|  | **Total Marks in Figures** | | | |  | **Total Marks in Words** | | |  | | |

**Q1. Provide Descriptive Answers of any FOUR (04) questions from the following: [08]**

1. **What is the difference between passive and active security threats?**
2. **What are the two general approaches to attacking a cipher?**
3. **What is the difference between diffusion and confusion?**
4. **List and briefly define types of cryptanalytic attacks based on what is known to the attacker.**
5. **Which parameters and design choices determine the actual algorithm of a Feistel cipher?**
6. **List and briefly define categories of passive and active security attacks.**
7. An attacker attempts to change the content of the communications in Active Attack. Whereas in the Passive attack, the communications are observed by an attacker, copied and used for malicious purposes.
8. First is “Brute force attacks” which consists of attempting any possible code, mix or password before the correct one is identified and second is “Cryptanalysis” which can be done by ciphertext statistical modeling.
9. Confusion refers to making the relationship as complicated and entangled as possible between the ciphertext and the symmetric key while Diffusion refers to the dissipation of the plaintext statistical structure over the ciphertext bulk.
10. **Active Attacks:**

Masquerade: Masquerade attack takes place when one entity pretends to be different entity

Modification of messages: This means that any part of a message has been changed or that

message has been postponed or reordered to create an unauthorized result.

**Passive Attacks :**

The release of message content

Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information.

Analysis of traffic

Suppose we had a way to mask (encrypt) content, so that the attacker could not retrieve any information from the packet, even though the message was intercepted.

**Q2 (a). Which security mechanism (s) are provided in each of the following cases: [02]**

1. A university server disconnects a student if he is logged into the system for more than two hours
2. A bank requires customer signature for a withdrawal
3. Access Control mechanism would be use in this case to terminate session of long hold student.
4. Digital Signature security mechanism would be used in order to prevent an entity from denying an action took place

**Q2 (b). Which technique (Cryptography or Steganography) is used in each of the following cases for confidentiality: [02]**

1. a student writes the answers to a test on a small piece of paper, rolls up the paper, and inserts in a ball-point pen and passes the pen to another student
2. a company uses special ink on its cheques to prevent forgeries
3. **Steganography**
4. **Cryptography**

**Q3 (a). Affine cipher is not vulnerable to frequency analysis. Do you agree or disagree? Justify your answer. [02]**

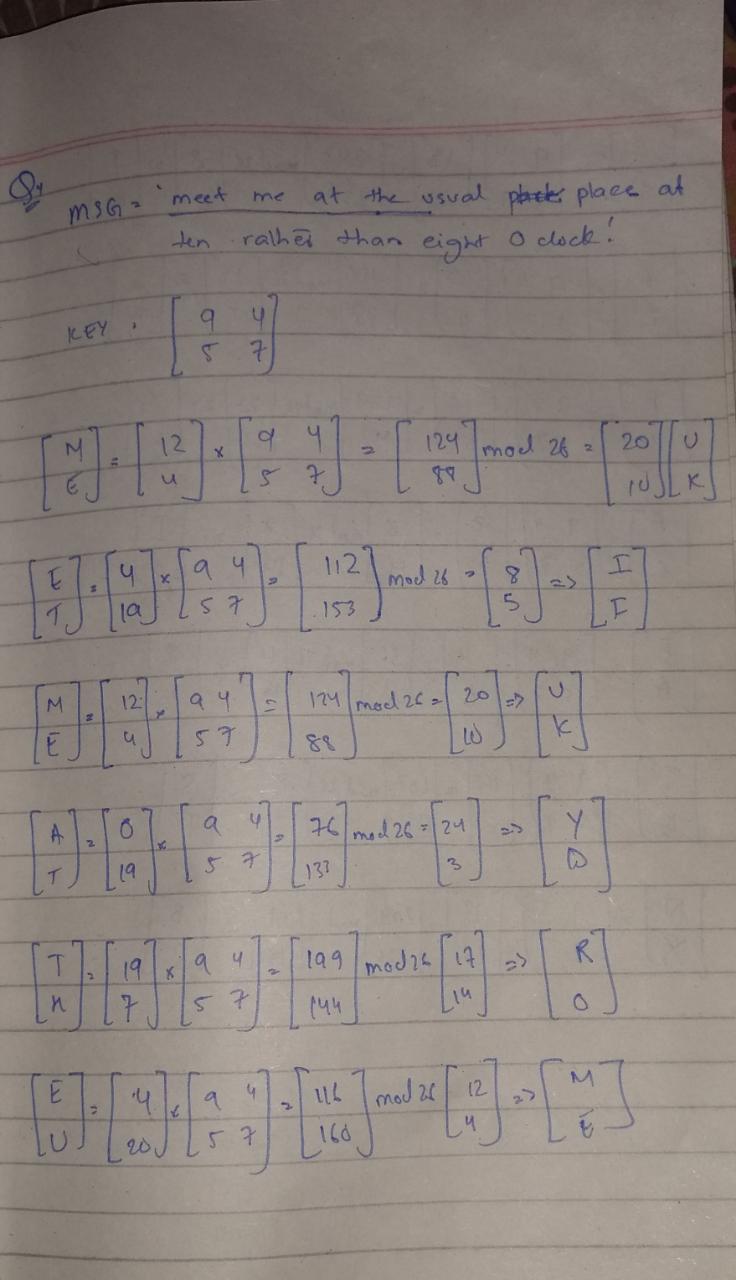
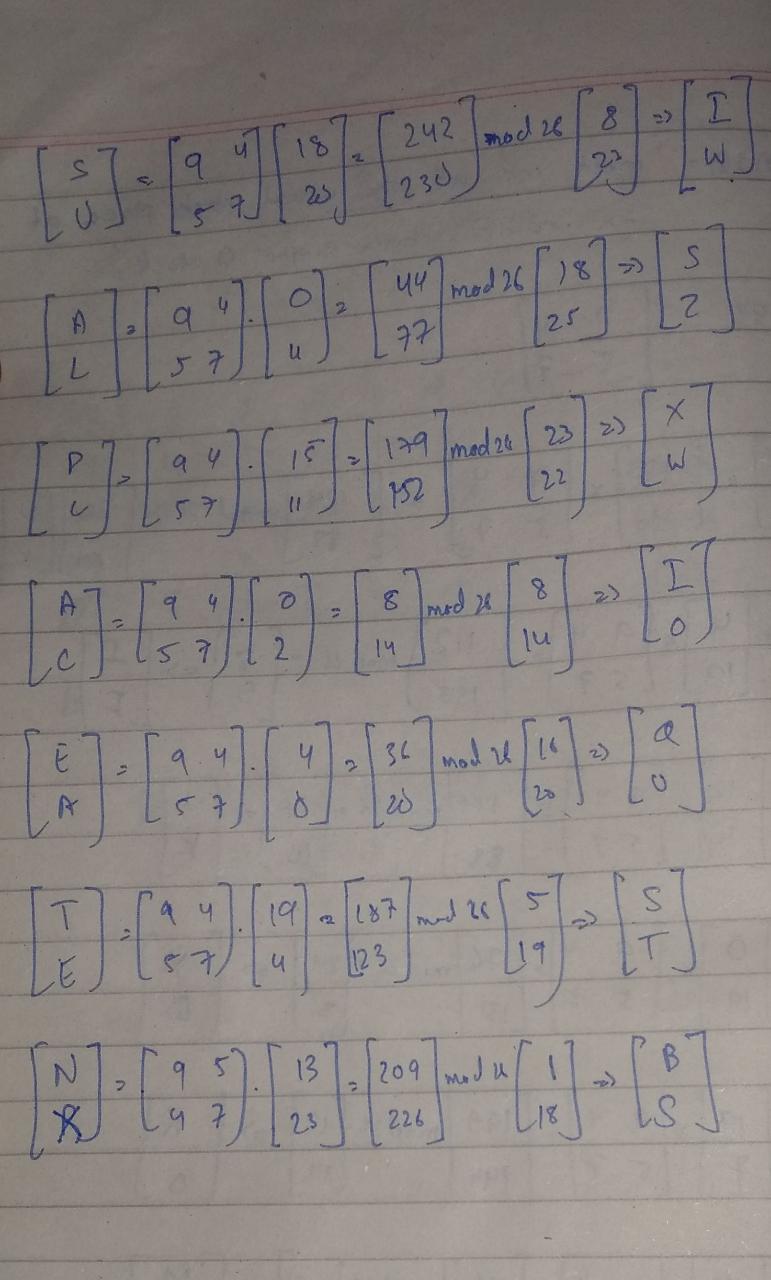
The cipher is less reliable than a substitution cipher because, in addition to other attacks, it is vulnerable to all the attacks that operate against substitution ciphers. The primary drawback of the cipher stems from the fact that if the cryptanalyst can uncover the plaintext of two ciphertext characters (via frequency analysis, brute force, guessing or otherwise), then the key can be retrieved.

**Q3 (b). Affine cipher is an example of polyalphabetic cipher. Do you agree or disagree? Justify your answer. [02]**

**YES,** Affine cipher is a type of monoalphabetic cipher as it’s each letter in an alphabet is translated to its numerical counterpart, it is encrypted and transformed back to a letter using a basic mathematical function.

**Q4. Encrypt the message "meet me at the usual place at ten rather than eight oclock" using the Hill cipher with the below key. Show your calculations and the result. [05]**



Cipher Text is : UKIFUKYDROMEIWXZXWIOQUSTBS

Plain Test : **meet me at the usual place at ten (due to time constraint)**

**Q5. When an American patrol boat was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code: [05]**

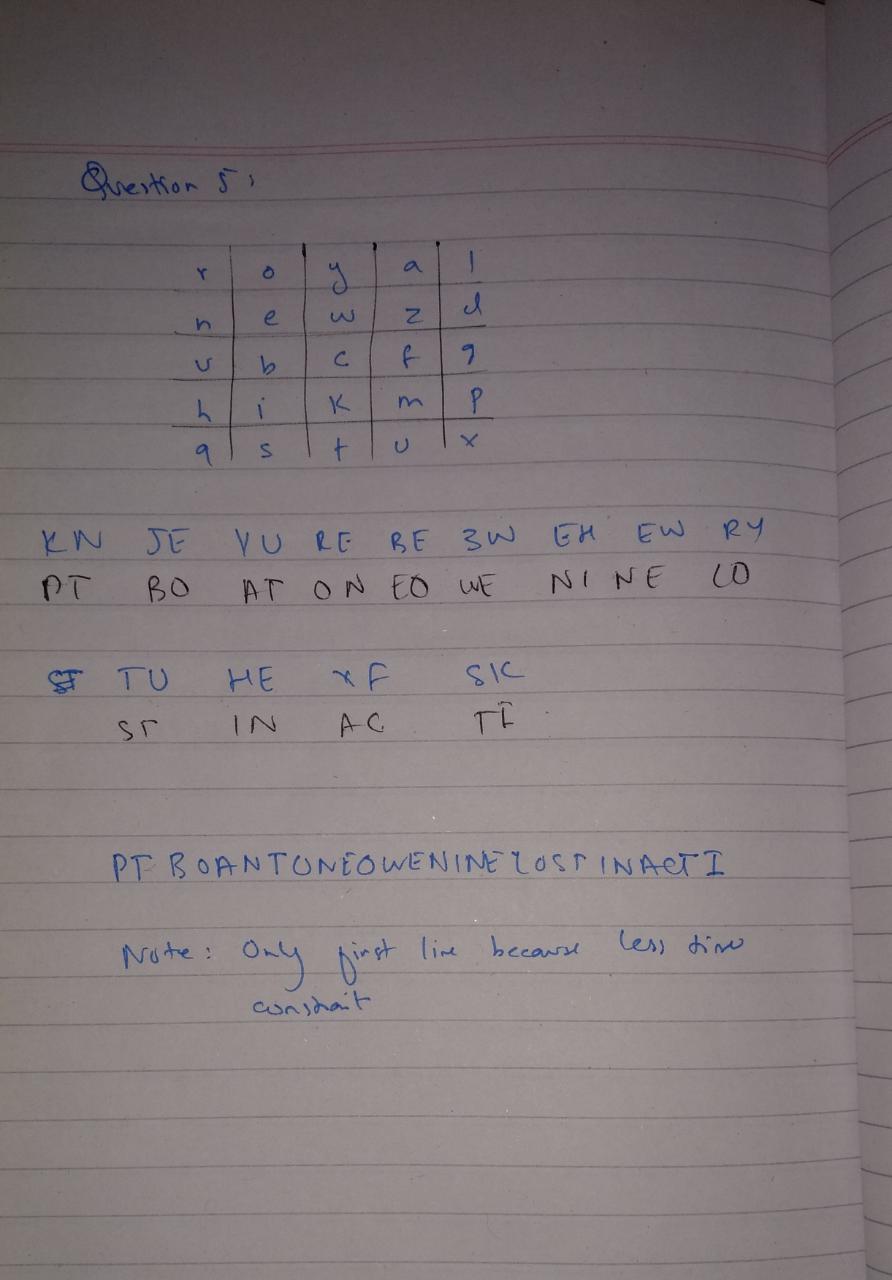
KXJEY UREBE ZWEHE WRYTU HEYFS

KREHE GOYFI WTTTU OLKSY CAJPO

BOTEI ZONTX BYBNT GONEY CUZWR

GDSON SXBOU YWRHE BAAHY USEDQ

The key used was *royal new zealand navy*. Decrypt the message. Translate TT into tt.



**Q6. Ahsan has a long message to send. He is using the monoalphabetic substitution cipher. He thinks that if he compresses the message, it may protect the text from single-letter frequency attack by attackers. Does the compression help? Should he compress the message before the encryption or after the encryption? Defend your answer. [04]**

Compression changes the entropy of the files, unlike the monoalphabetic substitution cipher. The encrypted data would then have the same entropy as the compressed data when a monoalphabetic substitution cipher is added to the compressed data. As such, on this evidence, an attacker would not be able to perform a frequency analysis. This is because they are oblivious of what entropy is.