# CIS7 Unit 11 In-Class Assignment: Cryptograph and Modular Arithmetic

This assignment is based on Chapter 5 concepts. Refer to textbook and Chapter 5 notes to complete the below exercises.

1. Based on Caesar Cipher, a substitution cipher, encrypt the following messages by ***shifting the letters 7 places to the right***. Input the shifted characters in the 2nd row of each table, then encrypt the message.
2. COMPUTER SCIENCE = JVTWBALY ZJPLUJL

| 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 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

1. KEEPING SECRETS = RLLWPUN ZLJYLAZ

| 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 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

1. CHANGE THE WORLD = JOHUNL AOL DVYSK

| 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 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

1. Using the same technique, decrypt the following messages using Caesar Cipher by ***shifting the letters 7 places to the left***. Input the shifted characters in the 2nd row of each table, then decrypt the message.
2. ZBJJLZZMBS WYVALJAPVU = SUCCESSFUL PROTECTION

| 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 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

1. LUJVKPUN ALEA = ENCODING TEXT

| 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 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

1. Encode the below messages using the provided table using double digits from 00 - 25, as described in Chapter 5. We will use 26 for a space, 27 for a period and 28 for a comma.
2. TAKE ON CHALLENGES

190010042614132602070011110413060418

| A | B | C | D | E | F | G | H | I | J | K | L | M |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

1. TOP SECRET

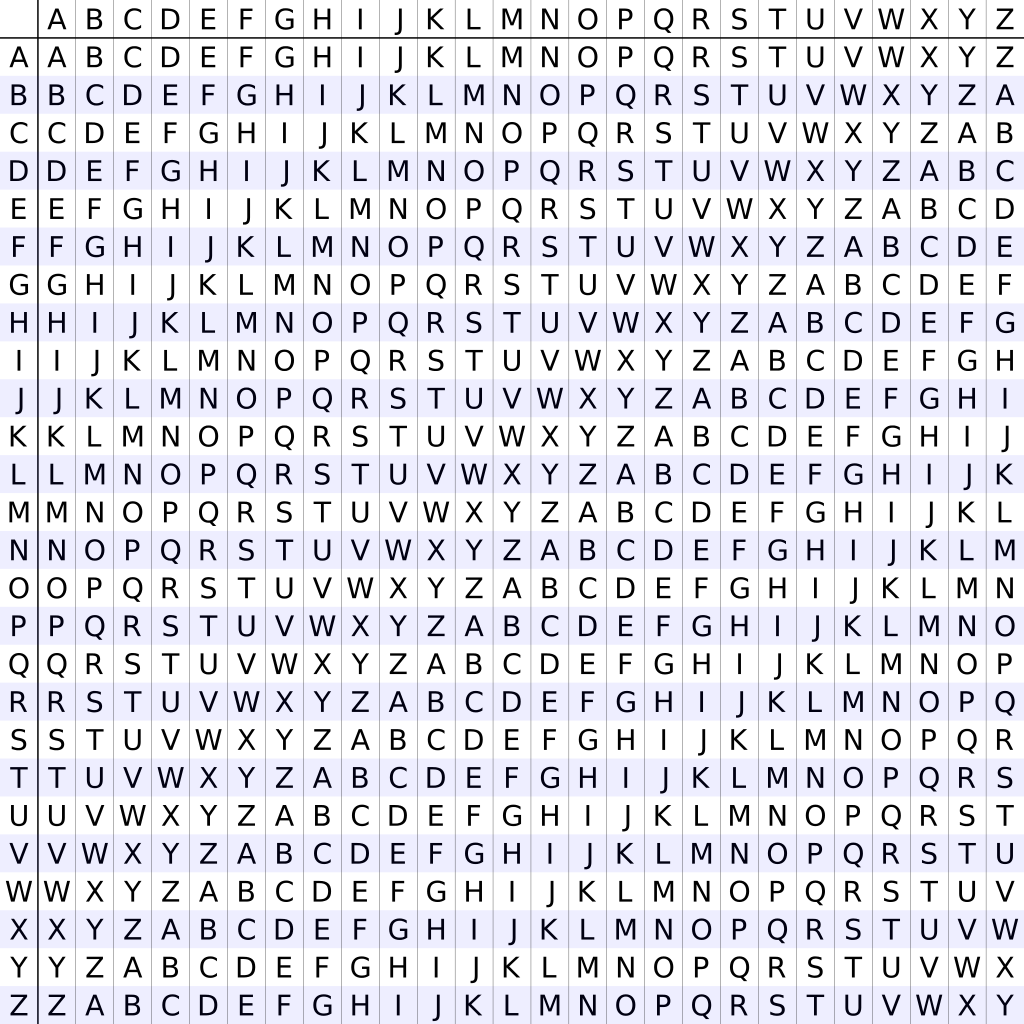
19141526180402170419

| A | B | C | D | E | F | G | H | I | J | K | L | M |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

1. Describe the One-Time Pad Ciphering method.

Uses random key, key is as long as message that is sent and received. Sender and receiver both hold the key. It’s ideal for one-time use.

1. Using Vigenere cipher and determine the encrypted message for the below phrases and keyword?



1. PLAIN TEXT: GRADUATIONISNEAR

KEY: EARNEARNEARNEARN

CIPHER: KRRQYAKVSNZFRERE

1. PLAIN TEXT: MASKPLAINTEXT

KEY: SECRETSECRETS

CIPHER: EEUBTESMPKIQL

1. Refer to Chapter 5 mod function definition, examples and solve for the following problems:
2. 80 mod 3

80 / 3 = 26 remainder 2

1. 120 mod 14

120 / 14 = 8 remainder 8

1. 975 mod 2

975 / 2 = 487 remainder 1

1. 461 mod 3

461 / 3 = 153 remainder 2

1. 726 mod 25

726 / 25 = 29 remainder 1

1. Given (A + B) mod C = (A mod C + B mod C) mod C , solve the following problems:
2. (15+16) mod 7

(15 % 7 + 16 % 7) % 7 = 3

1. (10 + 29) mod 4

(10%4 + 29%4) % 4 = 3

1. (19 + 23) mod 8

(19 % 8 + 23 % 8) % 8 = 2

1. Given (A \* B) mod C = (A mod C \* B mod C) mod C, solve the following problems:
2. (18\*11) mod 5

(18 % 5 \* 11 % 5) % 5 = 3

1. (33 \* 22) mod 4

(33 % 4 \* 22 % 4) % 4 = 2

1. (15 \* 27) mod 2

(15 % 2 \* 27 % 2) % 2 = 1

1. Given **ammod n = (amodn)m,** solve the following problems:
2. 46mod 3

(4%3)^6 % 3 = 1

1. 183mod 7

(18%7)^3 % 7 = 1

1. 224mod 9

(22%9)^4%9 = 4