VIT-AP UNIVERSITY

Programme: MTSE Semester: Winter 2020-21

Subject: Information and System Security Subject Code: SWE3003

ASSIGNMENT-1

Marks (Weightage) : 20 (8%) **Submission Due Date: 28-Mar-2021**

[**Note**: You may use computer programs to solve. But show detailed steps of the solutions.]

1. Draw a matrix like the Table (relationship between security services and mechanisms) that shows the relationship between security services and attacks.
2. Draw a matrix similar to the Table (relationship between security services and mechanisms) that shows the relationship between security mechanisms and attacks.
3. Find integer x such that
   a. $5x \equiv 4 \pmod 3$ b) $7x \equiv 6 \pmod 5$ c) $9x \equiv 8 \pmod 7$
4. Prove the following:
   a. $a \equiv b \pmod n$ and $b \equiv c \pmod n$ imply $a \equiv c \pmod n$
   b. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
   c. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$
5. Show that an integer N is congruent modulo 9 to the sum of its decimal digits. For example, $475 \equiv 4 + 7 + 5 \equiv 16 \equiv 1 + 6 \equiv 7 \pmod 9$.
6. Break the following ciphertext
   "PELCGBTENCULVFSBEVASBEZNGVBAFRPHEVGL" which is generated by monoalphabetic additive substitution cipher.
7. Break the ciphertext "UNTWXEAPUWNUGGKSYXK" which is generated by monoalphabetic multiplicative substitution cipher.
8. The affine Caesar cipher works as follows.
   $C=E([K_1, K_2], P) = P * K_1 + K_2$ $P=D([K_1, K_2], C) = (C - K_2) * K_1^{-1}$

A basic requirement of any encryption algorithm is that it be one-to-one. That is, if $p \neq q$, then $E(k, p) \neq E(k, q)$. Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is **not one-to-one** for all values of $\mathbf{K_1}$. For example, for $K_1 = 2$ and $K_2 = 3$, then $E([K_1,K_2], 0) = E([K_1,K_2], 13) = 3$.

(a) Determine which values of K_1 are not allowed.

(b) Are there any limitations on the value of K_2? Explain.

9. Decrypt the message "XICKGLTIZKSCRHUFM" by considering the monoalphabetic substitution scheme as a b c ... x y z ➔ Z Y X ... C B A.

10. Break the ciphertext "MTMTCMSALHRDY" which is generated using Auto-key cipher.

11. Alice and Bob use Playfair cipher for sending messages.

(a) Alice encrypted the plaintext "hello bob come soon" and sent to Bob. The key used is "VITAPBC$" (replace $ with your specialization, e.g., D/E/N). What is the ciphertext received by Bob?

(b) What is the plaintext decrypted by Alice if Bob sent the ciphertext "EOZAIQLNPVLW" using the key "VITAP"?

12. Encrypt the message "solve the assignment individually" with the key "**$**VITAP" using columnar transposition cipher. (Replace $ according to your specialization as mentioned in the below table). Find the Decryption key and decrypt the ciphertext to get the plaintext.

Note: Encoding the key can be done using sequence of characters in the alphabet. For example:

Specialization	**$**
Artificial Intelligence	L
Data Analytics	D
Computer Science	S
NW & Security	Y

Key (String)	**Key (Numeric)**
LVITAP	[3 6 2 5 1 4]
DVITAP	[2 6 3 5 1 4]
SVITAP	[4 6 2 5 1 3]
YVITAP	[6 5 2 4 1 3]

13. Alice sent the ciphertext "TPQSPIZYRRRRCZRGYIOAEPAEEETZCOHUMRC" using keyed-columnar transposition cipher with encryption key [5 3 2 4 1]. Decrypt the plaintext.

14. This problem explores the use of a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 ..., then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

(a) Encrypt the plaintext "send more money" with the key stream [9 0 1 7 23 15 21 14 11 11 2 8 9].

(b) Using the ciphertext produced in part a, find a key so that the cipher text decrypts to the plaintext "CASHNOTNEEDED".

15. Encrypt the message "meet me at the usual place at ten rather than eight o clock" using the Hill cipher with the key $\begin{bmatrix} 9 & 5 \\ 4 & 7 \end{bmatrix}$. Show your calculations and the result. Also show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

16. Decipher the message YITJP GWJOW FAQTQ XCSMA ETSQU SQAPU SQGKC PQTYJ using the Hill cipher with the inverse key $\begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix}$. Show your calculations and the result.

17. Decipher the message MWALO LIAIW WTGBH JNTAK QZJKA ADAWS SKQKU AYARN CSODN IIAES OQKJY B using the Hill cipher with the inverse key $\begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix}$. Show your calculations and the result.

18. Encrypt the plaintext P (your registration number) using the Hill cipher. The key $[K]$ should be also your registration number. [Note: Consider Z_{13}={0,1,…,9, M, I, S}]

For example, $K = P = 20MIS7123 = \begin{bmatrix} 2 & 0 & M \\ I & S & 7 \\ 1 & 2 & 3 \end{bmatrix}$.

Show your calculations and the result. Also show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

---$---