EMU – Faculty of Arts and Sciences

Department of Mathematics

****

COMP434 Cryptography and Network Security

Final Examination

Answer keys

****

Question 1. Given a plaintext message $p = (p_1, p_2, \dots)$ where p_i is a letter in some alphabet and invertible $m \times m$ matrix H, Hill cipher represents p_i by numeric value $x_i \in \mathbb{Z}_n (\mathbb{Z}_n = \{0,1, \dots, n-1\})$ and encrypts plaintext as $y = H \cdot x \ (mod\ n)$, where x and y are plaintext and ciphertext column vectors. Similarly, y is decrypted as $x = H^{-1} \cdot y \ (mod\ n)$. Consider a scenario where a cryptanalyst can break the system and obtain matrix H. Which parameters of the system and at which capacity should be known to guess H? What matrix operation could be performed to recover H?

Answer

Hill cipher can be obviously broken, knowing only m distinct plaintext and ciphertext pairs (x, y) and by computing $H = Y \cdot X^{-1} \ (mod\ n)$, where X and Y are the matrices composed of m columns of x and y, respectively. Whenever X is invertible the opponent can obviously compute the unknown key as $H = Y \cdot X^{-1} \ (mod\ n)$ and consequently break the cipher. If the X is not invertible then cryptanalyst keeps on collecting m plaintext and ciphertext pairs until the resulting matrix is invertible. When m is unknown, cryptanalyst might try the procedure for $m = 2,3,4$ until the key is found.

Question 2: Encryption with double columnar transposition technique with permutation 4312567 results in ciphertext NSCY AUOP TTWL TMDN AOIE PAXT TOKZ. Decrypt the ciphertext.

Solution

We enter ciphertext according to the key 4312567 columnwise and read output rowwise from left to right and from up to down.

2nd columnar transposition

4	**3**	**1**	**2**	**5**	**6**	**7**
T	T	N	A	A	P	T
M	T	S	U	O	A	O
D	W	C	O	I	X	K
N	L	Y	P	E	T	Z

1st columnar transposition

4	**3**	**1**	**2**	**5**	**6**	**7**
A	T	T	A	C	K	P
O	S	T	P	O	N	E
D	U	N	T	I	L	T
W	O	A	M	X	Y	Z

Plaintext: ATTACKPOSTPONEDUNTILTWOXYZ

Question 3: Suppose that you are computing an RSA key pair.

(a) What are p and q and $\psi(n)$ for an $n = 51$?

(b) Find a legal RSA public key pair for this p and q.

(c) How many possible values for e are there?

Solution

(a) The two factors of n are 3 and 17. Thus, $p = 3$, $q = 17$and $\psi(n) = (p-1)(q-1) = 2 \times 16 = 32$.

(b) $\gcd(e, 51) = 1$. An example of $e = 5$. $5d \equiv 1 \ mod \ 51 \Rightarrow d = 41$.

(c) There are 31 possible values for e. All these values are indicated in white cells.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Question 4: Suppose Alice sends authenticated secret message to Bob. Bob authenticates the same plaintext while keeping Alice's digital signature on it. Then Bob sends the secret message,

which is authenticated by Alice and himself, to Cathy. On receipt of the secret message Cathy reads it and gets sure that the message is authenticated by Alice and Bob. Let private and public keys used by Alice, Bob and Cathy are represented by KR_A, KU_A, KR_B, KU_B, KR_C and KU_C, respectively, and let X stand for the plaintext, write a sequence of actions performed by Alice, Bob and Cathy in pseudomathamatical form.

Solution

$Y = E_{KU_B}(E_{KR_A}(X))$ is a confidental message authenticated by Alice and sent to Bob.

$Z = E_{KU_C}(E_{KR_B}\left(E_{KR_A}(X)\right)$ is confidential message authenticated by Bob and Alice and sent to Cathy.

$X = D_{KR_C}(D_{KU_B}\left(D_{KU_A}(Z)\right)$ is plaintext which Cathy decrypts with Bob and then Alice's public keys.

Question 5: Give brief description of Shannon's confusion and diffusion principles.

Solution

In diffusion, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits; generally, this is equivalent to having each ciphertext digit be affected by many plaintext digits. On the other hand, confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key.