**NAME: DABO LAURA I.**

**MATRIC NUMBER: 16/SCI01/053.**

**COURSE CODE: CSC 418.**

**COURSE TITLE: INFORMATION SYSTEMS SECURITY.**

**ASSIGNMENT TITLE: REVISED QUESTIONS PART III.**

**START DATE: 08-06-2020.**

**END DATE: 01-07-2020.**

**QUESTION**

Kindly use these questions to revise the topics we have treated so far. It will come in batches, this is the third batch. The rest will be posted as times goes on. Kindly attempt it and submit online.

1. Write short note on the following:
2. Chosen-ciphertext attack
3. Chosen – key attack
4. Rubber – hose cryptanalysis
5. There is no code that cannot be broken and there is no algorithm that is secured, justify.
6. Write short note on Brute-force attack.
7. Given the following plaintext, encrypt it using Caesar cipher. Plaintext: corona virus is killing around the world
8. Decipher the following ciphertext, given C = E(7,p) = p+7 mod26. JYFWAVWYHWOF PZ UVA AVV KPMMPJBSA
9. Given the following plaintext and the ciphertext, 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 M O R S A T V E Y Z P N X D G U B L W C Q J F H K I
10. What type of cipher is this?
11. Decipher the following ciphertext: RMD KGQ OA XK TLYADS.
12. Encrypt the following plaintext: I JUST CANNOT BREAK YOUR CODE
13. Write short note on play-fair cipher
14. Using the play-fair technique encrypt the following plaintext given HORIZONTAL as the key: SIMPLE SUBSTITUTION H O R I/J Z N T A L B C D E F G K M P Q S U V W X Y
15. Using the play-fair technique encrypt the following plaintext given RECEIVER as the key: SIMPLE SUBSTITUTION R E C I V A B D F G H K L M N O P Q S T U W X Y Z
16. In vigenere cipher, encrypt this given plaintext: “keep it secret” using “unbreakable” as the key.

**ANSWER**

1. Chosen-ciphertext attack: The cryptanalyst can choose different ciphertexts to be decrypted and has access to the decrypted plaintext. E.g. the cryptanalyst has access to a tamper proof box that does automatic decryption. His job is to deduce the key.
2. Chosen – key attack: This attack does not mean that the cryptanalyst can choose the key; it means that he has some knowledge about the relationship between different keys. Note that it is strange and obscure, not very practical.
3. Rubber – hose cryptanalysis: The cryptanalyst threatens, blackmails or tortures someone until they give him the key. Bribery is sometimes referred to as a purchase key attack. These are all very powerful attacks and often the best way to break an algorithm.
4. The best algorithms are the ones that is made public, that have been attacked by the world’s best cryptographers for years and are still unbreakable. Good cryptographers rely on peer review to separate the good algorithms from the bad. An algorithm is unconditionally secure if no matter how much ciphertext a cryptanalyst has, there is not enough information to recover the plaintext that is,
5. The cost of breaking the cipher exceeds the value of the encrypted information.
6. The time required to break the cipher exceeds the useful lifetime of the information.
7. In Brute-force attack, the attacker tries every possible keys on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible key must be tried to achieve success. In this attack, if the message is English then the result pops out easily if a message is compressed before encryption then recognition becomes more of generate type of data such as a numerical file and has been compressed, the problem is even more difficult to automate. Therefore to supplement the brute force approach, some degree of knowledge about the expected plaintext is needed and some means of automatically distinguishing plaintext from garble is also needed.
8. Plaintext: corona virus is killing around the world

Using a shift of 3

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext Alphabet | 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 |
| Ciphertext Alphabet | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

**Ciphertext: FRURQD YLUXV LV NLOOLQJ DURXQG WKH ZRUOG**

Using a shift of 1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext Alphabet | 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 |
| Ciphertext Alphabet | 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 |

**Ciphertext: DPSPOB WJSVT JT LJMMJOH BSPVOE UIF XPSME**

1. C = E(7,p) = p + 7 mod 26.

Ciphertext: JYFWAVWYHWOF PZ UVA AVV KPMMPJBSA

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext Alphabet | 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 |
| Ciphertext Alphabet | 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 |

**Plaintext: cryptopraphy is not too difficult**

1. Decipher: **CAN YOU BE MY FRIEND**
2. **Y ZQWC RMDDGC OLAMP KGQL RGSA**
3. In play-fair cipher scheme, pairs of letters are encrypted, instead of single letters as in the case of simple substitution cipher. A key table is created first. The key table is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table as we need only 25 alphabets instead of 26. If the plaintext contains J, then it is replaced by I.

The sender and the receiver deicide on a particular key, say ‘tutorials’. In a key table, the first characters (going left to right) in the table is the phrase, excluding the duplicate letters. The rest of the table will be filled with the remaining letters of the alphabet, in natural order. The key table works out to be:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T | U | O | R | I |
| A | L | S | B | C |
| D | E | F | G | H |
| K | M | N | P | Q |
| V | W | X | Y | Z |

1. Plaintext: SIMPLE SUBSTITUTION

Key: "HORIZONTAL"

After split: SI MP LE SU BS TI TU TI ON

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| H | O | R | I | Z |
| N | T | A | L | B |
| C | D | E | F | G |
| K | M | P | Q | S |
| U | V | W | X | Y |

**Ciphertext: QZ PQ AF KY GY LO NV LO HT**

1. Plaintext: SIMPLE SUBSTITUTION

Key: "RECEIVER"

After split: SI MP LE SU BS TI TU TI ON

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| R | E | C | I | V |
| A | B | D | F | G |
| H | K | L | M | N |
| O | P | Q | S | T |
| U | W | X | Y | Z |

**Ciphertext: YF KS KC OY FP SV OZ SV TH**

1. Key: “unbreakable”

Plaintext: “keep it secret”

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key | u | n | b | r | e | a | k | a | b | l | e |
| Numeric representation | 20 | 13 | 1 | 17 | 4 | 0 | 10 | 0 | 1 | 11 | 4 |

Key numeric representation: 20 13 1 17 4 0 10 0 1 11 4

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext | k | e | e | p | i | t | s | e | c | | r | | e | t |
| Key | u | n | b | r | e | a | k | a | b | l | | e | | u |
| Numeric representation | 20 | 13 | 1 | 17 | 4 | 0 | 10 | 0 | 1 | | 11 | | 4 | 20 |
| Ciphertext | E | R | F | G | M | T | C | E | D | | C | | I | N |

**Ciphertext: ERFG MT CEDCIN**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key | u | n | b | r | e | a | k | a | b | l | e |
| Numeric representation | 21 | 14 | 2 | 18 | 5 | 1 | 11 | 1 | 2 | 12 | 5 |

Key numeric representation: 21 14 2 18 5 1 11 1 2 12 5

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Plaintext | k | e | e | p | i | t | s | e | c | r | e | t |
| Key | u | n | b | r | e | a | k | a | b | l | e | u |
| Numeric representation | 21 | 14 | 2 | 18 | 5 | 1 | 11 | 1 | 2 | 12 | 5 | 21 |
| Ciphertext | F | S | G | H | N | U | D | F | E | D | J | O |

**Ciphertext: FSGH NU DFEDJO**