**Ryan Carey**

**IST 454**

**Professor Rawel**

**1)Draw the Symmetric Cryptosystem diagram. (15 points)**

**A close up of a mans face

Description automatically generated**

1. **To protect the security of a Symmetric Cryptosystem, the good guys should \_\_\_\_\_\_\_\_\_ (10 points)**

**(c) Protect the attacker from knowing the key**

1. **Suppose the character set and positions of characters are given by:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Position** | | | **0** | | **1** | | **2** | **3** | | **4** | | **5** | | **6** | | **7** | | **8** | **9** | | **10** | | **11** | | **12** | |
| **Character** | | | **A** | | **B** | | **C** | **D** | | **E** | | **F** | | **G** | | **H** | | **I** | **J** | | **K** | | **L** | | **M** | |
| **13** | **14** | **15** | | **16** | | **17** | | | **18** | | **19** | | **20** | | **21** | | **22** | | | **23** | | **24** | | **25** | |  |
| **N** | **O** | **P** | | **Q** | | **R** | | | **S** | | **T** | | **U** | | **V** | | **W** | | | **X** | | **Y** | | **Z** | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Now let’s use position-based substitution to decrypt message: CATTIGER**

**(2.1) If the secret key is: SUN, what is the plaintext?  Please show the decryption process. (25 points)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| C = 2 | A = 0 | T = 19 | T = 19 | I = 8 | G = 6 | E = 4 | R = 17 |
| S = 18 | U = 20 | N = 13 | S = 18 | U = 20 | N = 13 | S = 18 | U = 20 |
| (2+26)-18 = 10 = K | (0+26)-20 = 6 = G | 19-13 = 6 = G | 19-18 = 1 = B | (8+26)-20 = 14 = O | (26+6)-13 = 19 = T | (4+26)-18 = 12 = M | (17+26)-20 = 23 = X |

**Plaintext = KGGBOTMX**

1. **If the plaintext is “HORSELSP” and the block size is 5, what is the key? (25 points)**

**Key = Cyphertext - Plaintext**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| C = 2 | A = 0 | T = 19 | T = 19 | I = 8 | G = 6 | E = 4 | R = 17 |
| H = 7 | O = 14 | R = 17 | S = 18 | E = 4 | L = 11 | S = 18 |  |
| (2+26)-7 = 21 = V | (0+26)-14 = 12 = M | 19-17=2 = C | 19-18=1 = B | 8-4=4 = E | (26+6)-11 = 21 = V | (4+26)-18 = 12 = M |  |

**Key = VMCBE**

1. **Say True or False to the following statement and explain WHY (25 points): “Chosen-ciphertext cryptanalysis” means that the attacker can choose the set of cipher-texts he is going to use to break the code, but the attacker does not know any plaintext since the cryptanalysis is not “chosen-plaintext cryptanalysis.”**

False, the attacker does know some plaintext and is working backwards to try and figure out the key knowing both the cyphertext and some plaintext.