Issa Odeh

CS 454 M2 questions

09/03/2021

Q1. The ciphertext below was encrypted using a substitution cipher. Decrypt the ci-phertext without knowledge of the key.

lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk lmird jk xjubt trmui jx ibndt wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

1. Compute the relative frequency of all letters A...Z in the ciphertext. You may want to use a tool such as the open-source program CrypTool for this task. However, a paper and pencil approach is also still doable.

   A=5 , B=68, C=5, D=23, E=5, F=1, G=1, H=23, I=41, J=48, K=49, L=8, M=92, N=17, O=7, P=30, Q=7, R=84, S=17, T=13, U=24, V=22, W=47, X=20, Y=19, Z=0.

2. Decrypt the ciphertext with the help of the relative letter frequency of the English language. Note that the text is relatively short and that the letter frequencies in it might not perfectly align with that of general English language from the table.

   because the practice of the basic movements of kata is the focus and mastery of self is the essence of matsubayashi ryu karate do i shall try to elucidate the movements of the kata according to my interpretation based on forty years of study it is not an easy task to explain each movement and its significance and some must remain unexplained to give a complete explanation one would have to be qualified and inspired to such an extent that he could reach the state of enlightened mind capable of recognizing soundless sound and shapeless shape i do not deem myself the final authority but my experience with kata has left no doubt that the following is the proper application and interpretation i offer my theories in the hope that the essence of okinawan karate will remain intact

3. Who wrote the text? Shoshin Nagamine

Q2. We now consider the relation between passwords and key size. For this purpose we consider a cryptosystem where the user enters a key in the form of a password.

1. Assume a password consisting of 8 letters, where each letter is encoded by the ASCII scheme (7 bits per character, i.e., 128 possible characters). What is the size of the key space which can be constructed by such passwords?

   Answer = 128^8 or 2 ^56

2. What is the corresponding key length in bits?

   Answer = 56

3. Assume that most users use only the 26 lowercase letters from the alphabet instead of the full 7 bits of the ASCII-encoding. What is the corresponding key length in bits in this case?

   Answer: 26 ^8

Q3. As we learned in this chapter, modular arithmetic is the basis of many cryptosystems. As a consequence, we will address this topic with several problems in this and upcoming chapters. Let's start with an easy one: Compute the result without a calculator.

15 · 29 mod 13 = **15 mod 13 * (29 mod 13)*mod 13**

= 2 * (29 mod 13) mod 13

= 2 * 3 mod 13

= 6 mod 13

= 6

$2 \cdot 29 \bmod 13$ = **2 mod 13 * (29 mod 13) mod 13**

= 2 * 3 mod 13

= 6 mod 13

= 6

$2 \cdot 3 \bmod 13$ = **2 mod 13 * (3 mod 13) mod 13**

= 2 * 3 mod 13

= 6 mod 13

= 6

$-11 \cdot 3 \bmod 13$ = **-11 mod 13 * (3 mod 13) * mod 13**

= 2 * 3 mod 13

= 6

The results should be given in the range from 0,1,..., modulus-1.

Q4. We conduct a known-plaintext attack on an LFSR-based stream cipher. We know that the plaintext sent was: 1001 0010 0110 1101 1001 0010 0110 By tapping the channel we observe the following stream: 1011 1100 0011 0001 0010 1011 0001

1. What is the degree m of the key stream generator?

   Using XOR gate we get the code sequence 0010 1110 0101 1100 1011 1001 0111

   Then rearrange into 7 blocks: 0010111 0010111 0010111 0010111 0010111

$M = Log_2(P+1)$

In this case, P = 7 since the key repeats every 7 bits.

M= 3

2. What is the initialization vector?

   S0 = 0, S1 = 0, S2 = 1

   Turns into

   (S2 =1, S1 = 0, S0 = 0)

3. Determine the feedback coefficients of the LFSR.

   S2P2 + S1P1 + S0P0 = S3

   S3P2 + S2P1 + S1P0 = S4

   S4pP2 + S3P1 + S2P0 = S5

   Now substitute vales from number 2 we get:

   1p2 + 0p1 + 0p0 = 0 = s3

   0p2 + 1p1 + 0p0 = 1 = s4

   1p2 + 0p1 + 1p0 = 1 = s5

   Now we construct a matrix:

1	0	0	0
0	1	0	1
1	0	1	1

   Turns into:

1	0	0	0
0	1	0	1
0	0	1	1

4. Draw a circuit diagram and verify the output sequence of the LFSR.