Fall 2022 2022-09-14

Solutions for Assignment 1

Roopa Vishwanathan *CS 380/525: Intro to Crypto*

1. Caesar cipher – same as answer 2. For a generic shift cipher, ask for the encryption of any single plaintext character, say m, and let c be the ciphertext returned, Once you get c, just do $k = c - p(\text{mod}128)$.

   For a generic substitution cipher, choose a plaintext containing 127 ASCII characters, same reasoning as answer 2. For Vigenere, same as answer 2. One thing to bear in mind is when using the 128-character ASCII set is that the frequency chart used should be appropriate too, i.e, there should be frequencies for lowercase letters, whitespace, etc., not just case-insensitive alphabets. Only Caesar cipher and Vigenere is asked, generic shift/substitution not needed in answer.

2. For the Caesar, actually no plaintext is required, since its just a shift by 3, the key is already known. Just shift each letter of the ciphertext left by 3 places. For a generic shift cipher (of unknown shift value), ask for the encryption of any single plaintext character, say m, and let c be the ciphertext returned, Once you get c, just do $k = c - p(\text{mod}26)$.

   For a generic substitution cipher with a random mapping between alphabets, choose a plaintext containing 25 letters of the English alphabet (easily generalizes to other alphabets too). You can figure out the last alphabet yourself, since the mapping will be unique per letter. In practice, though you might need less, using a dictionary and frequency table.

   For Vigenere cipher, if the key length is known, say k, ask for the encryption of a plaintext of length k. If the key length is not known, it is a bit more challenging. Assuming you know the upper bound on the length of the key, k_{max}, ask for an encryption of a plaintext of length k_{max}. Only Caesar cipher and Vigenere is asked, generic shift/substitution not needed in answer.

3. The tag is computed thus: $Tag \leftarrow MAC(K, M)$, and sent along with the ciphertext, $C \leftarrow E_K(M)$. Charlie can modify C in transit to say, C', and he can also modify the Tag to say, Tag'. But there will be no correspondence between the C' and Tag'. Since the Tag' was just some randomly created string, and key K was not used in the creation of it.

   Bob will do $M' \leftarrow D_K(C')$, but the next step will fail: $Tag' \neq MAC(K, M')$.

4. CBC mode:

   (a) See class written notes for figure, pg. 17-18.

   (b) The equations for encryption are as follows:
   $C_1 = E_K(IV \oplus M_1)$,
   $C_2 = E_K(C_1 \oplus M_2)$,
   $C_3 = E_K(C_2 \oplus M_3)$,
   $C_4 = E_K(C_3 \oplus M_4)$,
   $C_5 = E_K(C_4 \oplus M_5)$.

So, the equations for decryption are:
$M_1 = D_K(C_1) \oplus IV$,
$M_2 = D_K(C_2) \oplus C_1$,
$M_3 = D_K(C_3) \oplus C_2$,
$M_4 = D_K(C_4) \oplus C_3$,
$M_5 = D_K(C_5) \oplus C_4$.
Charlie has changed C_1 to C_1'. Bob's first decryption will be: $M_1' = D_K(C_1') \oplus IV$, which is wrongly decrypted. His second decryption will be: $M_2' = D_K(C_2) \oplus C_1'$, which is also wrongly decrypted. His third decryption will be: $M_3 = D_K(C_3) \oplus C_2$, which is correctly decrypted. All decryptions from this point on do not need C_1'. So all subsequent decryptions will be correct.

So, Bob cannot correctly decrypt M_1, M_2. All other blocks are correctly decrypted by him.

Note that there is no "partial/fractional decryption" of an individual block. A given block is either decrypted correctly or wrongly.

(c) The equations for encryption/decryption are the same as above. IV is mangled to IV'. Bob does: $M_1' = D_K(C_1) \oplus IV'$, which is wrongly decrypted. His second decryption will be: $M_2 = D_K(C_2) \oplus C_1$, which is correctly decrypted. $M_3 = D_K(C_3) \oplus C_2$, which is also correctly decrypted. All decryptions from this point on do not need IV'. So all subsequent decryptions will be correct.

So, Bob cannot decrypt M_1 correctly, but all other blocks will be decrypted correctly by him.