Exercise 1 (2023)

Test

1. Mutual index of coincidence of strings 'abab' and 'cbcb' is ......
2. Index of coincidence of string 'abab' is ......
3. Unicity distance of plaintext decreases with decreasing entropy of the key.

   □ yes □ no
4. The two-time pad problem is an issue in what block-cipher mode?

   □ CBC □ OFB □ ECB
5. The time complexity of the meet-in-the-middle attack on triple encryption with three independent keys is $\sim 2^X$, where X is

   □ n □ $2n$ □ $3n$ □ $4n$
6. Slide attack requires that the attacker can choose plaintexts (CPA).

   □ yes □ no
7. Which mode usually employs padding?

   □ CBC □ OFB □ CFB □ CTR
8. GCM mode of authenticated encryption uses for encryption "part"

   □ CBC □ OFB □ CFB □ CTR
9. The private exponent d in RSA scheme and $\varphi(n)$ are coprime.

   □ yes □ no
10. The Chinese remainder theorem is used in RSA scheme to speed up encryption.

    □ yes □ no
11. If we can efficiently solve DLOG problem in a group, then we can efficiently solve the computational Diffie-Hellman problem in this group.
    □ yes □ no
12. Ciphertext in the ElGamal scheme is a pair (r, s). Which of these values depend on the plaintext?
    □ both □ only r □ only s □ neither

Problems

1. Describe the slide attack on a variant of Speck-$2n$ cipher, in which we use the same encryption key in each round. The length of the key is n bits and the number of rounds is n. What is the time and memory complexity of this attack – compare it with the brute-force attack? Can you improve the attack in the CPA setting?

2. Propose a ciphertext stealing for ECB mode. We assume that the plaintext is longer than one block. We expect (1) number of E_k calls for encryption does not change; (2) there will be no XOR operation. Describe encryption and decryption for your proposal.

3. We use AES in CFB mode with a padding (e.g. PKCS #7 padding), even though it is not necessary. Describe how oracle padding attack works in this case and what an attacker achieves with the attack.

4. The determinism of "textbook" version of RSA scheme is viewed as a weakness. Analyze the security of the following modifications that use a randomization factor $r \overset{\$}{\leftarrow} Z_n^*$. Encryption of a plaintext $m \in Z_n$ is

   (a) $(r^e \bmod n, r + m \bmod n)$;
   (b) $(r, (rm)^e \bmod n)$.

5. Find the smallest interval that contain unicity distance for Vigenere cipher with key length 4, if the alphabet of the plaintext language contains 32 letters.