Symmetric Key Cryptography Optional Worksheet (for self-study)

1. Alice and Bob have decided to use the Vigenère cipher to send private emails to each other. At their last meeting in person, they exchanged a 6 character word to be used as the secret key for the Vigenère cipher. Marvin, their adversary, intercepted the following encrypted email content sent by Alice to Bob:

   `VXUWPFSTRWINHHBFCPZDVSOYWRX`

   Marvin suspects that Alice usually begins her emails to Bob with the greeting `HIBOB` and has overheard that the key is 6 letters. He heard that the Vigenère cipher is vulnerable to known plaintext attacks, and would like to exploit this weakness to decrypt Alice's message.

   (a) Explain how Marvin can exploit a known plaintext attack to determine some information (or all) on Alice and Bob's secret key.

   (b) Find the secret key using the above data available to Marvin.

   (c) Use the information obtained in previous step to decrypt Alice's email to Bob.

2. Does a substitution need to be a permutation of the plaintext symbols? Why or why not?

3. **Attack Models:** In the security community, the security of any security scheme is typically analyzed with respect to attack models, which formally define two aspects:

   - security goal (the attacker's goal will be the opposite of this)
   - adversarial capability

   (a) **Security goal** Differentiate between the different variants of security goals that could be considered for CONFidentiality: infeasibility of key recovery (KR), infeasibility of plaintext recovery (PR), indistinguishability (IND)

      i. Discuss which security goal is the strongest (hardest to achieve by the security defender, easiest to achieve by the attacker).

      ii. Hence, explain why (give brief arguments) the goal you identified above is the strongest security goal.

   (b) **Adversarial capability:** Discuss the different types of adversarial capabilities that have so far been considered in the security literature, e.g. ciphertext-only attack (COA), known-plaintext attack (KPA), chosen plaintext/ciphertext attack (CPA/CCA), including which one is the strongest capability and why.

   (c) **Attack:** Choose one of the encryption schemes you have learnt or are aware of, or you can google for more.

      i. Explain a simple attack that can be mounted on this encryption scheme.

      ii. Explain which attack model (what security goal, what adversarial capabilities) is required and relevant for this attack.

   (d) **Defend:** Now switch sides and wear the security defender's hat.

      i. Discuss why this attack was possible, what weakness it exploited, what adversarial capability was required by the attacker.

      ii. Could we change the attack model to cause this attack to no longer be valid? e.g. we only consider an attack model with weaker adversarial capabilities, or we only consider an attack model with a weaker security goal.

      iii. Then discuss how this attack can be prevented, e.g. could the encryption scheme be tweaked to resist attacks in this model?