COM-301 Computer Security

Exercise sheet: Applied Cryptography

1. Decrypt the following ciphertext encrypted using the Caesar cipher (we have removed the spaces):

   ULCLYBZLAOLJHLZHYJPWOLY

2. For each of the following scenarios, decide whether it represents a Known Plaintext Attack (KPA), a Chosen Plaintext Attack (CPA), or Neither. Briefly justify your answer.

   (a) Eve intercepts an encrypted email and guesses that it begins with the header "From:".

   (b) Eve gains temporary access to Alice's encryption device and asks it to encrypt the string "abcdefghijklmnopqrstuvwxyz".

   (c) Eve passively listens to ciphertexts on the network but has no knowledge of the plaintexts and cannot influence them.

   (d) Eve interacts with a company's encryption API, submitting arbitrary strings and receiving their ciphertexts.

   (e) Eve tries to guess Bob's password directly by logging in with common passwords.

3. Consider the OTP encryption scheme. In the correct OTP, the key K is as long as the message and used only once, which guarantees perfect secrecy. However, suppose the scheme is implemented incorrectly: a fixed 4–bit key K is chosen and then repeated over and over to encrypt a long message M using XOR.

   (a) Suppose Eve has temporary access to the encryption device and can submit any plaintext of her choice. Show how she can recover the repeated 4–bit key K with a single chosen plaintext query. Which adversary model does this correspond to?

   (b) Now suppose Eve does not control the plaintext, but she knows that the messages always begin with the same 8 characters, and she knows the values of these characters. Can she still recover the key in this case? If yes, explain how, and identify the adversary model.

4. Alice and Bob want to agree on a shared secret using the Diffie–Hellman (DH) protocol. They publicly agree on:

$$p = 23, \quad g = 5.$$

Alice chooses secret exponent $a = 6$, and Bob chooses secret exponent $b = 15$.

   (a) Compute the public values. Calculate Alice's public value $A = g^a \bmod p$ and Bob's public value $B = g^b \bmod p$.

   (b) Compute the shared secret. Show how Alice and Bob each compute the shared secret K, and verify that both arrive at the same value.

   (c) Which mathematical problem ensures that Eve, who sees p, g, A, B, cannot easily compute K?

5. What happens if an adversary has the ability to intercept a Diffie Hellman key exchange between Alice and Bob? Can the adversary read Alice and Bob messages? (hint: think about the man-in-the-middle concept). If Alice and Bob have each a pair (SK,PK) of signing keys, and they know each other's public keys. Can you solve the problem?