COM-301 Computer Security
Exercise sheet: Applied Cryptography

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

   ULCLYBZLAOLJHLZHYJPWOLY

   Solution:
   The shift is 7 and the text reads: "Never use the Caesar cipher"

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.

   Solution:

   (a) KPA: Eve knows part of the plaintext ("From:") and its ciphertext.

   (b) CPA: Eve chooses a plaintext and obtains its ciphertext.

   (c) Neither: This is passive eavesdropping without known or chosen plaintext.

   (d) CPA: Eve can query an encryption oracle with chosen plaintexts.

   (e) Neither: This is a password guessing attack, not a cryptanalytic KPA/CPA.

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.

   Solution:

   (a) This is a CPA. Eve can submit the plaintext $M = 0000$. The ciphertext output will be $C = M \oplus K = K$, which directly reveals the 4–bit key.

   (b) Yes, even partial knowledge of the plaintext is enough. If Eve knows that the first four plaintext bits are 0101 and sees the corresponding ciphertext (say 0110), she can compute $K = M \oplus C = 0101 \oplus 0110 = 0011$. This is a KPA: knowing just part of the plaintext–ciphertext pair suffices to recover the repeated key.

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?

   Solution:

(a) Public values. With $p = 23$ and $g = 5$:

$$A = 5^6 \bmod 23 = 8, \quad B = 5^{15} \bmod 23 = 19.$$

(b) Shared secret. Alice computes $K_A = B^a \bmod 23 = 19^6 \bmod 23 = 2$. Bob computes $K_B = A^b \bmod 23 = 8^{15} \bmod 23 = 2$. Thus $K_A = K_B = 2$.

(c) Security assumption. Security relies on the *Discrete Logarithm Problem (DLP)*: given g, p, and $A = g^a \bmod p$, it is infeasible to recover a. Computing $K = g^{ab} \bmod p$ from only g^a and g^b is the Computational Diffie–Hellman problem, assumed hard.

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?

Solution:
The adversary can intercept the public key sending, and send a key of her own to Alice and Bob. This way she establishes a shared secret with Alice, and a shared secret with Bob, while both Alice and Bob think they are speaking with each other.

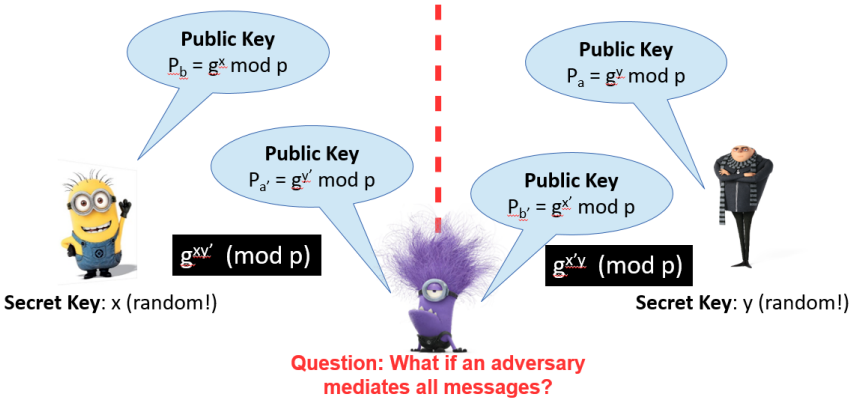

Figure 1: Diffie Hellman key exchange interception.

Then when she sees a message from Alice, she decrypts it with the shared key Alice-adversary, and encrypts it with the shared key Bob-adversary. She reads all the messages without Alice and Bob being aware.

If Alice and Bob have signing keys, they can sign the value they send to each other. Thus, even if the adversary intercepts the messages, she

cannot mediate. This is because, as she does not know the secret keys, she cannot impersonate Alice nor Bob – i.e., she cannot establish secrets with Alice (resp. Bob) on Bob's behalf (resp. Alice).