Q1: Define Euler's Totient Function of a positive integer n with words.

A1: The number of non-negative integers less than n which are coprime to n.

Q2: Precicely describe how to calculate Euler's Totient Function of a positive integer n.

A2: First find the prime factorisation of n, call it $n = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdots {p_k}^{e_k}$. Next calculate the following to find $\phi(n)$:

$$\prod_{i=1}^{k} \left({p_i}^{e_i - 1} \cdot (p_i - 1) \right)$$

Q3: State Euler's Theorem.

A3: If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Q4: State Fermat's Little Theorem.

A4: If a is a positive integer and p is prime, then $a^p \equiv 1 \pmod{p}$.

Q5: What does it mean for a sett of integers to be pairwise coprime?

A5: The greatest common divisor of all the elements is 1.

Q6: State the Chinese Remainder Theorem.

A6: if $m_1, m_2, \cdots, m_r$ are pairwise coprime positive integers and $a_1, a_2, \cdots, a_r$ are integers, then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M := m1 \cdot m_2 \cdots m_r$ which is given by

$$x = \sum_{i=1}^{r} a_i M_i y_i \pmod{M}$$

where $M_i := M/m_i$ and $y_i :\equiv M_i^{-1} \pmod{m_i}$ for $1 \leq i \leq r$.

Q7: What is Kerckhoff's Assumption?

A7: Everything about a cryptographic system is public knowledge except for the key. In other words, the enemy knows the system.

Q8: Briefly explain the four levels of attacks on a cryptosystem, in ascending order of strength.

A8:

1. **Ciphertext only:** Opponent has access to some ciphertext and might use statistical information to determine the corresponding plaintext.
2. **Known plaintext:** Opponent knows some plaintext-ciphertext pairs and uses it to gain more knowledge of the key.
3. **Chosen plaintext:** Opponent is temporarily able to encrypt to build a collection of known plaintext-ciphertext pairs.
4. **Chosen plaintext-ciphertext:** Opponent is temporarily able to encrypt and decrypt.

Q9: What is the plaintext and ciphertext space of a shift cipher?

A9: Both are the non-negative integers less than 26.

Q10: Is a shift cipher a public or private system? What is/are the key(s)?

A10: Private. Key is the shift amount.

Q11: How do you encrypt a plaintext message with a shift cipher?

A11: Add the private key to the message modulo 26. In other words, rotate the letter by the key amount.

Q12: How do you decrypt a ciphertext message encrypted with a shift cipher?

A12: Subtract the private key from the message modulo 26. In other words, rotate the letter backwards by the key amount.

Q13: What are the best attacks for a shift cipher?

A13: Brute force (try every key) or analyse letter frequencies to determine the key.

Q14: What is the plaintext and ciphertext space for an affine cipher?

A14: Both are non-negative integers less than 26.

Q15: Is an affine cipher a public or private system? What is/are the key(s)?

A15: Private. The key is a pair of non-negative integers less than 26 where one of them is coprime to 26.

Q16: How do you encrypt a plaintext message with an affine cipher?

A16: Suppose the key is (a, b) where a is coprime with 26 and the message is x. To encrypt the message, calculate:

$$y \equiv ax + b \pmod{26}$$

Q17: How do you decrypt a ciphertext message encrypted with an affine cipher?

A17: Suppose the key is (a, b) where a is coprime with 26 and the encrypted message is y. The decrypt the message, calculate:

$$x \equiv a^{-1}(y - b) \pmod{26}$$

Q18: What are the best attacks for an affine cipher?

A18: Obtain two plaintext-ciphertext pairs and solve the resulting linear congruences for the key. Could also brute force. In otherwords, given x_1, y_1, x_2, y_2, solve the following for a and b.

$$y_1 \equiv ax_1 + b \pmod{26}$$
$$y_2 \equiv ax_2 + b \pmod{26}$$

You can also just try all combinations of a and b.

Q19:

A19:

Q20:

A20:

Q21:

A21:

Q22:

A22:

Q23:

A23: