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. To 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: What is the plaintext and ciphertext space for a mixed alphabet cipher?

A19: Both are non-negative integers less than 26.

Q20: Is a mixed alphabet cipher a public or private system? What is/are the key(s)?

A20: Private. The key is a permutation of the set of non-negative integers less than 26.

Q21: How do you encrypt a plaintext message with a mixed alphabet cipher?

A21: Suppose the key is a permutation of the set of non-negative integers less than 26, π and the message is x. To encrypt the message, calculate:

$$y = \pi(x).$$

Q22: How do you decrypt a ciphertext message encrypted with a mixed alphabet cipher?

A22: Suppose the key is a permutation of the set of non-negative integers less than 26, π and the encrypted message is y. To decrypt the message, calculate:

$$x = \pi^{-1}(y).$$

Q23: What are the best attacks for a mixed alphabet cipher?

A23: Use statistical analysis on the known language's letter frequencies. Can also search for common digrams and trigrams in the ciphertext which will correspond to things like "th", "he", "in", or "the", "ing", "and", etc. Piece together the key bit by bit.

Q24: What is the plaintext and ciphertext space for a Vigenère cipher?

A24: Both are strings of non-negative integers less than 26.

Q25: Is a Vigenère cipher a public or private system? What is/are the key(s)?

A25: Private. The key is a string of non-negative integers less than 26.

Q26: How do you encrypt a plaintext message with a Vigenère cipher?

A26: Suppose the key is a string of m non-negative integers less than 26, $k_1, k_2, \cdots k_m$. Further suppose the message is a string of m non-negative integers less than 26, $x_1, x_2, \cdots x_m$. To encrypt the message, calculate:

$$\begin{aligned} y_1 &\equiv x_1 + k_1 \pmod{26} \\ y_2 &\equiv x_2 + k_2 \pmod{26} \\ &\vdots \\ y_m &\equiv x_m + k_m \pmod{26} \end{aligned}$$

In other words, treat each element of the key and message as its own shift cipher and encrypt it accordingly.

Q27: How do you decrypt a ciphertext message encrypted with a Vigenère cipher?

A27: Suppose the key is a string of m non-negative integers less than 26, $k_1, k_2, \cdots k_m$. Further suppose the encrypted message is a string of m non-negative integers less than 26, $y_1, y_2, \cdots y_m$. To encrypt the message, calculate:

$$\begin{aligned} x_1 &\equiv y_1 - k_1 \pmod{26} \\ x_2 &\equiv y_2 - k_2 \pmod{26} \\ &\vdots \\ x_m &\equiv y_m - k_m \pmod{26} \end{aligned}$$

In other words, treat each element of the key and encrypted message as its own shift cipher and decrypt it accordingly.

Q28: What are the best attacks for a Vigenère cipher?

A28: Determine the key length, m, and break m shift ciphers independently using frequency analysis.

Q29: Name and explain one method to determine the key length of a Vigenère cipher.

A29: Kasiski's test. Find repeated trigrams in the ciphertext. If the key length is less than the number of occurrences of a trigram, then its corresponding plaintext must have been encrypted with the same shift more than once (by the Pigeonhole Principle).
We can then extract a common factor from the distances between the starting index of each repeated trigram to estimate the key length.

Q30: What is the index of coincidence of a language? How is it denoted?

A30: The probability of drawing two matching letters through random selection from a text in the given language. It is denoted with the greek letter φ (phi).

Q31: How do you calculate the index of coincidence for a language with n letters where the ith letter has probability of occurring p_i?

A31:

$$\sum_{i=1}^{n} p_i^2$$

Q32: What is the index of coincidence approximately equal to for English?

A32: 0.0667.

Q33: What is the index of coincidence equal to for a random language?

A33: $1/26 \approx 0.0384$.

Q34: Name and explain one method to determine the key length of a Vigenère cipher.

A34: Friedman's first method. Suppose your guess for the key length is m. Extract every mth letter from the ciphertext and calculate the index of coincidence of the extracted text. If it's close to the index of coincidence for English, it's probably the correct key length.

Q35: Name and explain one method to determine the key length of a Vigenère cipher.

A35: Friedman's second method. Calculate the index of coincidence for the entire ciphertext (φ_T) and use the measure of how "flat" is it compared with English (φ_L) and random text (φ_0) to estimate the key length.

$$m \approx \frac{\varphi_L - \varphi_0}{\varphi_T - \varphi_0}$$

Q36: What is the plaintext and ciphertext space for a Hill cipher?

A36: Strings of non-negative integers less than 26.

Q37: Is a Hill cipher a public or private system? What is/are the key(s)?

A37: Private. The key is a invertible matrix of non-negative integers less than 26.

Q38: How do you encrypt a plaintext message with a Hill cipher?

A38: Suppose the key is an invertible $m \times m$ matrix K and x is a message of length m. To encrypt the message, calculate:

$$y \equiv Kx \pmod{26}$$

Q39: How do you decrypt a ciphertext message encrypted with a Hill cipher?

A39: Suppose the key is an invertible $m \times m$ matrix K and y is an encrypted message of length m. To decrypt the message, calculate:

$$x \equiv K^{-1}y \pmod{26}$$

Q40: What are the best attacks for a Hill cipher?

A40: Obtain m plaintext-ciphertext pairs each of length m. Solve the resulting linear congruences for K:

$$\begin{aligned} y_1 &\equiv Kx_1 \pmod{26} \\ y_2 &\equiv Kx_2 \pmod{26} \\ &\vdots \\ y_m &\equiv Kx_m \pmod{26} \end{aligned}$$

Q41: How can we easily calculate Euler's Totient function of n where n is the product of two primes? In other words, how can we arrive at a simple expression for $\phi(pq)$?.

A41: We note that the prime factorisation of n is p^1q^1 so:

$$\phi(n) = \left[p^{1-1}(p-1)\right] \cdot \left[q^{1-1}(q-1)\right] = (p-1)(q-1)$$

Q42: What is the plaintext and ciphertext space for RSA?

A42: Both are non-negative integers less than the product of two primes.

Q43: Is RSA a public or private system? What is/are the key(s)?

A43: Public.

- The **public** key is (n, b) where n is the product of two **distinct** large primes p and q and b is a randomly chosen positive integer less than $\phi(n)$ (ϕ is Euler's Totient function) which is invertible modulo $\phi(n)$.
- The **private** key is (a, p, q) where a is $b^{-1} \pmod{\phi(n)}$ and p and q are the primes whose product makes n.

Q44: How do you encrypt a plaintext message with RSA?

A44: Suppose our public key is (n, b) and the message is x. To encrypt the message, calculate:

$$y \equiv x^b \pmod{n}.$$

Q45: How do you decrypt a plaintext message with RSA?

A45: Suppose our private key is (a, p, q) so $n = pq$ and our encrypted message is y. To decrypt the message, caclulate:

$$x \equiv y^a \pmod{n}.$$

Q46: What are the best attacks for RSA?

A46:

- If our private key has one prime much smaller than the other, we can easily factorise n.
- If our private key has primes roughly the same size, we can also easily factorise n.
- If the message to encrypt, x, is so small that $y := x^b \pmod{n}$ is less than n, then you can simply take the bth root of y over the reals to get back x.
- If the message to encrypt is predictable, simply try encrypting guesses and see if the resulting ciphertext matches.
- If the public exponent, b is so small that the same plaintext message is likely to be encrypted with b or more different keys, you can recover the plaintext using the Chinese Remainder Theorem.

Q47: Why is it important to sign and verify signatures of messages encrypted with public key cryptography?

A47: Because the public key of every sender is known, anybody can use the public key to encrypt any message and send to anybody. You need some claim of authenticity in the messages you send and receive.

Q48: How can a sender sign their RSA-encrypted message?

A48: Attach a signature to their encrypted message, which is a hashed plaintext encrypted with their private key rather than the public one. In other words, if the hashed message is $f(x)$ and the private exponent is a, the attaches the following signature to the ciphertext:

$$s \equiv (f(x))^a \pmod{n}$$

Q49: How can a receiver verify the signature of an RSA-encrypted message?

A49: Decrypt the signature, s, with the intended sender's public exponent, b, and see if it results in the hashed decrypted message $f(x)$. In other words, verify the following holds:

$$s^b \equiv f(x) \pmod{n}$$

Q50: How could a malicious sender send an encrypted message with RSA claiming to be somebody they're not.

A50: They obtain the public intended encrypted message and the signature and look for a collision in the hash function. They can then send their malicious encrypted message along with the original sender's signature and nobody will be able to detect foul play.

Q51: What is the plaintext and ciphertext space for ElGamal?

A51: Both are non-negative integers less than some large prime.

Q52: Is ElGamal a public or private system? What is/are the key(s)?

A52: Public.

- The **public** key is
- The **private** key is

Q53: How do you encrypt a plaintext message with ElGamal?

A53: ... To encrypt the message, caclulate:

$$blah$$

Q54: How do you decrypt a plaintext message with ElGamal?

A54: ... To decrypt the message, caclulate:

$$blah$$

Q55:

A55:

Q56:

A56:

Q57:

A57:

Q58:

A58:

Q59:

A59:

Q60:

A60:

Q61:

A61:

Q62:

A62:

Q63:

A63:

Q64:

A64:

Q65:

A65: