Answer: Kerckhoffs' Principle is a concept in cryptography that states a cryptographic system should be secure even if everything about the system, except the key, is public knowledge. This principle emphasizes that the security of a system should not rely on its algorithm being kept secret, but rather on the secrecy of the key used to encrypt and decrypt messages.

Modular arithmetic

- x = y mod N if and only if N divides x-y
- [x mod N] = the remainder when x is divided by N
  - I.e., the unique value $y \in \{0, \ldots, N-1\}$ such that x = y mod N

- 25 = 35 mod 10
- 25 ≠ [35 mod 10]
- 5 = [35 mod 10]

The Vigenère cipher

- The key is *multiple* characters, not just one
- To encrypt, shift each character in the plaintext by the amount dictated by the next character of the key
  - Wrap around in the key as needed
- Decryption just reverses the process

```
tellhimaboutme
cafecafecafeca
veqpjiredozxoe
```

Attacking the Vigenère cipher

- Look at every 14th character of the ciphertext, starting with the first
  - Call this the first "stream"
- Let α be the most common character appearing in this stream
- Most likely, α corresponds to the most common character of the plaintext (i.e., 'e')
  - Guess that the first character of the key is α - 'e'
- Repeat for all other positions

A better attack (high level)

- Let p_i ($0 \le i \le 25$) denote the frequency of the i^{th} English letter in normal English plaintext
  - One can compute that $\sum_i p_i^2 \approx 0.065$
- Let q_i denote the observed frequency of the i^{th} letter in a given stream of the ciphertext
- If the shift for that stream is j, expect $q_{i+j} \approx p_i$ for all i
  - So expect $\sum_i p_i q_{i+j} \approx 0.065$
- Test for every value of j to find the right one
  - Repeat for each stream

Threat models for encryption

- Ciphertext-only attack
  - One ciphertext or many?
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack

1. 唯密文攻击（Ciphertext-Only Attack）

- **定义**：攻击者仅能获取加密后的密文，但不知道对应的明文或密钥。这是最基础的攻击场景。

2. 已知明文攻击（Known-Plaintext Attack）

- **定义**：攻击者掌握部分明文及其对应的密文，目标是破解密钥或解密其他密文。

3. 选择明文攻击（Chosen-Plaintext Attack）

- **定义**：攻击者可以主动选择任意明文，并获取对应的密文，目标是推断密钥或解密其他密文。

4. 选择密文攻击（Chosen-Ciphertext Attack）

- **定义**：攻击者可以提交任意密文，并获取解密后的明文，目标是破解密钥或伪造合法密文。

Core principles of modern crypto

- **Formal definitions**
  - Precise, mathematical model and definition of what security means
- **Assumptions**
  - Clearly stated and unambiguous
- **Proofs of security**
  - Move away from design-break-patch cycle

The right definition

- “Regardless of any *prior* information the attacker has about the plaintext, the ciphertext should leak no *additional* information about the plaintext”