16 PEACE, JUSTICE AND STRONG INSTITUTIONS

GIRLS

Secure Communication for Whistleblowers

Authors

Luis Hernández Encinas, CSIC (Spain).
Agustín Martín Muñoz, CSIC (Spain).
Araceli Queiruga Dios, Universidad de Salamanca (Spain).

Type of activity

The problem presents an application of cryptography to solve the problem of secure communication, using basic modular arithmetic.

Target educational level

It can be addressed to last courses of High School students and to any university student from STEM degrees.

Initial information

Sustainable Development Goal 16, Target 16.10 emphasizes the importance of ensuring public access to information and protecting fundamental freedoms, in accordance with national legislation and international agreements. A critical aspect of this is protecting individuals who expose corruption or wrongdoing (whistleblowers), as their ability to communicate securely is paramount to their safety and the successful disclosure of vital information.

Imagine a scenario where a whistleblower, Alice, has sensitive information she needs to share with a journalist, Bob, without anyone else being able to intercept or read it. This requires a strong encryption method to guarantee both confidentiality and potentially authenticity (ensuring the message indeed came from Alice).

Source

Problem adapted from AI tool (Gemini).

Shanika Wickramasinghe, S. (2024). Caesar cipher features (link).

Koch, R. (2025). How to communicate securely with whistleblowers (link).

Problem statement

Alice, a whistleblower, needs to securely send a critical message to Bob, a journalist. They've agreed to use a symmetric encryption algorithm for speed and efficiency, specifically a Caesar cipher for this simplified example (though real-world scenarios would use much stronger algorithms like AES, RSA, EC, etc.).

The Caesar cipher works by shifting each letter of the plaintext a certain number of positions down or up the alphabet. For this problem, we'll use a numerical representation where $A = 0, B = 1, \ldots, Z = 25$.

Alice and Bob agree on a shared secret key (shift value) of $K = 5$. That secret message (plaintext) is: "EXPOSE".

Using the Caesar cipher rules and the agreed-upon key:

1. Encrypt the message "EXPOSE" to find the ciphertext Alice will send.
2. Demonstrate how Bob would decrypt the received ciphertext to recover the original message.

Solution:

1. Convert each letter of the plaintext "EXPOSE" into its numerical equivalent: $[E = 4, X = 23, P = 15, O = 14, S = 18, E = 4]$
2. Alice uses the encryption formula: $C_i = (M_i + K)(\mathrm{mod}\ 26)$, where C_i is the ciphertext number, M_i is the plaintext number, and K is the key (shift value). The modulo 26 ensures the result wraps around the alphabet (0-25).

   Applying the key $K = 5$ to each plaintext number, e.g., for $E\ = 4$, we have $(4 + 5)(\mathrm{mod}\ 26) = 9\ (\mathrm{mod}\ 26) = 9$. Doing the same for all letters, the ciphertext numbers are: $[9, 2, 20, 19, 23, 9]$.

   Converting these numbers back to letters: The ciphertext Alice sends is: "JCUTXJ".

3. For decrypting the ciphertext "JCUTXJ", Bob converts the ciphertext letters back into numbers (he knows the shared key $K = 5$):

$$[J = 9, C = 2, U = 20, T = 19, X = 23, J = 9].$$

Bob uses the decryption formula: $M_i' = (C_i - K)(\text{mod } 26)$, where M_i' is the decrypted plaintext number.

Applying the key $K = 5$ to each ciphertext number, e.g., for $J\ = 9$: we calculate $(9 - 5)(mod 26) = 4(mod 26) = 4$

Thus, the decrypted plaintext numbers are: [4, 23, 15, 14, 18, 4]

Converting these numbers back to letters, Bob successfully recovers the original message: "EXPOSE".