Peer Graded Assignment: Alice-Bob-Eve Framework using the Caesar Cipher

This assignment is to practice using the Alice-Bob-Eve framework. Identify a scenario when cryptography is used, e.g., online secure transactions or accessing a server data, and describe the context.

Let us take a simple case of a messaging application where Alice wishes to send Bob a message via this application and the contents of the message sent by Alice should be privy only to Alice and Bob.

Bob is on the other connected to the application via the internet and will receive the message from Alice. Eve is eavesdropping as usual and can see all the content flowing freely between Alive and Bob and wishes to understand the content of the messages that the 2 are sending amongst themselves.

In the scenario you identified, who is Alice? Bob? And Eve?

Alice and Bob are 2 users of the application who wish to share text messages with confidential information and do not want this information to be intercepted and understood. Eve is eavesdropping on the conversation and wishes to read and understand all the communication that is being interchanged between these parties.

What computations/operations do Alice and Bob perform for the cryptographic protection? State the concrete algorithm.

Alice and Bob are both using a Caesar cipher. That is they have a one-one surjective and injective mapping (bijective) for all the letters and alphabets. This mapping has simply been created by shifting the range of all alphabets by a constant and mapping the alphabets to this new range of characters.

So if we shift by 2 places

A → C

D → F and so on

And the number of shifts to create this mapping is known only by Alice and Bob and not eve.

A simple Java program that returns a string using a Caesar shift of r rotations :

```java
public static void main(String[] args) {
  System.out.println(caesarShift("anish sachdeva", 0));
  System.out.println(caesarShift("secret message", 3));
}


private static String caesarShift(String string, int shift) {
  StringBuilder accumulator = new StringBuilder();
  for (int index = 0 ; index < string.length() ; index++) {
     char character = string.charAt(index);
     accumulator.append((char) ((character + shift) % 128));
  }
  return accumulator.toString();
}
```

Alice will use this algorithm to Encrypt the data whereas Bob will use it to Decrypt data.

Identify an activity from Eve, which the cryptographic protection counters.

Alice is aware of the algorithm, but not the number of shifts, hence she can try shifting the cipher text multiple number of times, but then each time Alice will have to personally test the message whether it makes grammatical sense or not and this lack of information will make the task tedious for Alice.