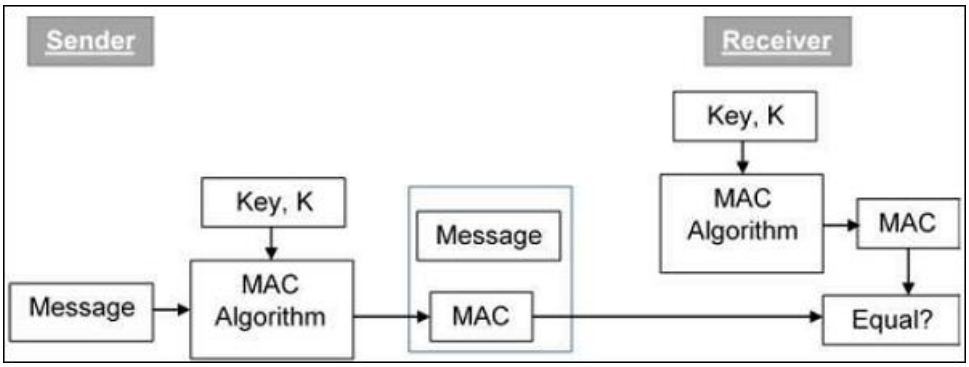
Java Security
MAC (Message Authentication Code)

- It is a symmetric key cryptographic technique to provide message authentication. For establishing MAC process, the sender and receiver share a symmetric key K.
- MAC is an encrypted checksum generated on the underlying message that is sent along with a message to ensure message authentication.
- In Java the Mac class of the javax.crypto package provides the functionality of message authentication code.




```
import java.security.Key;
import java.security.SecureRandom;

import javax.crypto.KeyGenerator;
import javax.crypto.Mac;

public class Test
{
	public static void main(String args[]) throws Exception{

	//Creating a KeyGenerator object
	 KeyGenerator keyGen = KeyGenerator.getInstance("DES");

	//Creating a SecureRandom object
	SecureRandom secRandom = new SecureRandom();

	//Initializing the KeyGenerator
	keyGen.init(secRandom);

	//Creating/Generating a key
	Key key = keyGen.generateKey();

	//Creating a Mac object
	Mac mac = Mac.getInstance("HmacSHA256");

	//Initializing the Mac object
	mac.init(key);

	//Computing the Mac
	String msg = new String("You have Oracle SLS.");
	byte[] bytes = msg.getBytes();
	byte[] macResult = mac.doFinal(bytes);

	System.out.println("Mac result:");
	System.out.println(new String(macResult));
  }
}
```

```
C:\Program Files\Java\jdk-11.0.12\bin\Manish>javac Test.java

C:\Program Files\Java\jdk-11.0.12\bin\Manish>java Test
Mac result:
?`~bQ¬9f??♥‼&↑E♠?T??%?i↓▲?:N?Q?ÿ
```