CYBERSECURITY E-DEGREE

SIGNATURE GENERATION USING HASH ALGORITHM

Using the following algorithms, generate a valid signature for the message 2.

- Hash function: (x+3) mod 10
- Encryption: RSA with the following parameters

- Private key: 11
- Public key: 5
- Modulus: 14

SOLUTION

Message = 2

Hash Function (which is to added to the message) = (x + 3) mod 10

Where x=2

The Hash Function is now = (2 + 3) mod 10

= 5 mod 10

This is the new message = 5 ← A

To get the encrypted message = 5^5 mod 14 = 3

Where 3 is the encrypted message and 5 in 5^5 is the public key

To get back the original message which is 5 (ARROW A above), we calculate:

3^{11} mod 14 = 5

Where 11 in 3^{11} is the private key and 3 is the encrypted message