Feedback on Topic 4 Ex

Exercise Question – E4.1 - Q

Name three application scenarios or cases where using RSA is preferable than using AES and name one application scenario where the use of AES is necessary.

Exercise Question – E4.1 - A

- Scenarios for using RSA (Public-key cipher)
  - Two or more communication entities have not established an AES key.
  - Communication/interacting entities do not trust each other.
  - One entity needs to send out a signed document to another entity, or message authentication and non-repudiation protection is required.
- Scenarios for using AES (Symmetric-key cipher)
  - The encryption of video or other stream/real-time/bulk data.

Exercise Question – E4.2 - Q

You are a recipient of p = 5, q = 7. You make the modulus n = 35 public. You also choose an exponent e = 5 and make that public too.

Messages are sent to you, one letter at a time. Letters are coded into numbers as: A -> 0, B -> 1, and so on.

Now, the following message has arrived for you:

17 19 7 9 0 12 24

Decrypt this message.

Exercise Question – E4.2 - A

n=p*q=35;

phi=(p-1)*(q-1)=4*6=24;

e=5, so e*d = 1 mod 24 → e*d=24*k+1, where k are integers. We need to find the smallest integer of d that satisfies this equation, which is 5.

Take the first letter, 17,

$M=17^{d}$ mod 35 = 17^{5} mod 35 = (((((17*17) mod 35) *17 mod 35)*17 mod 35)*17) mod 35 = 12 mod 35, so the first letter in the received message is ‘m’.

Using the same method, we can get the plaintext: ‘my heart’.