**Quiz 3/6**

**Q)**

1. **Asymmetric cryptography algorithms and their two major differences and major applications?**
2. **Suppose the difficulty bits is 5. Then make this puzzle 16 times more difficult, then how many more difficult bits? (Nonce project)**

**A)**

The two major differences in asymmetric cryptography algorithms like RSA and Elliptic Curve Cryptography (ECC) are going to be the key size and performance for encryption and decryption.

Key sizes for algorithms are

| **RSA** | **ECC** |
| --- | --- |
| at least 2048 Bits | Range from 160 to 521 bits |

Performance is the speed and efficiency of the encryption and decryption processes.

| **RSA** | **ECC** |
| --- | --- |
| is Slow compared to other algorithms | Faster and more efficient than RSA |

The two major applications are

1. Encryption and Decryption

| Plain text → Cipher Text | Cipher Text → Plain Text |
| --- | --- |
| **Public key** | **Private Key** |

1. Digital Signature

To verify the authenticity of the information sent and also ensure the integrity of the data being transmitted.

Creating a new puzzle with 16 times the difficulty is possible by counting the number of more difficult bits required, which is 42 = 16.

We can increase it to 9

Probability of winning nonce when 5 = 1 out of 32

Probability of winning nonce when 9 = 1 out of 512