|  |  |
| --- | --- |
| Symmetric Cipher | Block Cipher Operation, Pseudorandom Number Generator and Stream Ciphers (RC4) |
| Asymmetric Ciphers | Public Key Cryptography, RSA, Diffie Hellman Key Exchange, Elgamal cryptosystem |
| Number Theory | CRT, Properties of multiplicative group,  Fermat little theorem, Euler function, Primality Testing – Miller Rabin Algorithm, Discrete logarithms |

**T2 Syllabus**