CS847

Not Registered this time.

**Reconfigurable Architectures for Cryptographic Algorithms** **3 credit**

**UNIT 1**

Introduction to modern cryptography- secret key cryptography-Hash functions- Public key Cryptography-Digital Signature Schemes- Fundamental operations for cryptographic algorithms- design alternatives for implementation.

**UNIT 2**

FPGAs- Xilinx and Altera FPGAs- comparison with ASIC and general purpose processor- Design Flow and parallelism- security in reconfigurable hardware devices.

**UNIT 3**

Finite Fields – Binary finite fields - Elliptic curves- Elliptic curves over $GF(2^m)$ – point representation – projective coordinates – Lopez- Dahab coordinates -Scalar representation – recoding methods and ω-NAF representation.

**UNIT 4**

Prime finite field arithmetic – addition operation – different adder modules – modular addition operation – Omura's method - modular multiplication operation – Brickell's method and Montgomery's method – modular exponentiation operation.

**UNIT 5**

MD5- message preprocessing- MD buffer initialization - Final transformation SHA-1,SHA-256, SHA-384 and SHA -512 – Hash computations - hardware architectural designs – iterative design – pipelined design – unrolled design – mixed approach.

**References:**


1. Francisco Rodriguez-Henriquez N.A. Saqib A. Diaz-Perez, "Cryptographic Algorithms on Reconfigurable Hardware", Springer, 2006.
2. William Stallings, "Cryptography and network security: principles and practice", 6th edition, Pearson Education, 2013.


Senate RR

76

Devipriya 10611 70070 CSE

Dr. M. Brinda CSE