PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

Welcome to

PES University

Ring Road Campus, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES
UNIVERSITY

APPLIED CRYPTOGRAPHY

Lecture 3

Basic Cryptographic Primitives

Building blocks

Cryptographic primitive

- Cryptographic primitives are well-established, low-level cryptographic algorithms that are frequently used to build cryptographic protocols for computer security systems.

Cryptographic protocols

- Used for secure application-level data transport
- Incorporates the following aspects
    - Key agreement or establishment
    - Entity authentication
    - Symmetric encryption and message authentication material construction
    - Non-repudiation methods
    - Secret sharing methods
    - Secure multi-party computation
    - Examples: IPsec, Kerberos, Secure Shell (SSH) etc..,

Cryptographic primitives

- Mainly divided as
  - Unkeyed primitives
  - Symmetric-key primitives
  - Public-key primitives

Unkeyed primitives

- Unkeyed includes
  - Hashing, SHA-family
  - One-way permutations
- Use
  - Hash and sign

Simmitric – key primitive

- Single key shared between sender and receiver
- Design principles
  - Block size
  - Key size
  - Number of rounds
  - Subkey generation
  - Round function
  - Fast software en/decryption

Symmetric- key primitives

- Block ciphers
- Stream ciphers, RC4 - also can come from
- Mode of block ciphers
- PRNG - pseudo-random number generators

Public key primitives

- Participant possesses a private and a public key.
    - Message encrypted from public key can be decrypted using private key
    - Message encrypted from private key can be decrypted using public key
- Main ingredients of public key system:
    - Plaintext
    - Encryption algorithm
    - Private key
    - Public key
    - Decryption algorithm
    - Ciphertext

Public key primitives

- Public-key cryptosystems
- Signatures
- PKI - public-key infrastructure, only if we had it right :-(

Math in primitives

- Keyless: so far mostly bit swapping
- Shared-key:
  - Mostly around binary Galois fields GF(2^k)
- Public-key: mostly use number theory,
  - Now essentially in all Public key cryptography, including ECC

Math in cryptanalysis

- Probability and statistics, random oracle models
- Number theoretical algorithms: primality, factoring
- Discrete logarithms: cyclic group discovery, index calculus,
- counting points on elliptic curves, theory of elliptic curves

Cryptographic primitive evaluation

- Primitives should be evaluated with respect to various criteria such as:
    - Level of security - is usually difficult to quantify.
    - Functionality - primitives will need to be combined to meet various information security objectives.
    - Mode of operation - primitives, when applied in various ways and with various inputs, will typically exhibit different characteristics.
    - Performance - refers to the efficiency of a primitive in a mode of operation.
    - Ease of implementation – refers to the difficulty of realizing the primitive in a practical instantiation.

Next Class

☞ Mandatory reading for the next class

https://ieeexplore.ieee.org/document/1455525
http://ciphermysteries.com/other-ciphers/blitz-ciphers

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU Center for Information Security, Forensics and Cyber Resilience

PESU Center for Internet of Things