CPE 633
Chapter 9 – Fault Detection in Cryptographic Systems

Dr. Rhonda Kay Gaede

UAH

Motivation

- Cryptographic algorithms are used to provide high levels of security using _____ hardware.
- This hardware has a high _____ to faults.
- _____ _____ is a technique used to find cryptographic keys.

9.1 Overview of Ciphers

- Cryptography
  - Plain text ⇒ Cipher text (_____)
  - Cipher text ⇒ Plain text (_____)
- Keys
  - Symmetric
    - Distributed Securely
  - Public/Private
    - Sender _____ needed

9.1.1 Symmetric Key Ciphers

- Symmetric key ciphers can be either _____ ciphers or _____ ciphers.
- _____ ciphers are more commonly used
  - Data Encryption Standard (DES) – __-bit blocks, __-bit keys
  - Advanced Encryption Standard (AES) – ___-bit blocks, ___-___-bit keys
- The main objective of the encryption process is to _____ the plaintext as much as possible using _____ of _____.
- Two crucial properties for good ciphers
  - _____ – _____ _____ between plaintext and the key
  - _____ – eliminate natural _____ or _____ found in plaintext

9.1.2 Public Key Ciphers

- Much more computationally _____ than _____ keys
- May be used for _____ _____
- Key generation process consists of finding _____ _____ numbers with at least a _____ digits

9.2 Security Attacks Through Fault Injection

- Security of ciphers relies on the fact that _____ searches taking a _____ amount of time are required to find the secret key
- _____ _____ attacks exploit _____ information
  - _____ _____ may be related to the ____ of the key.
  - _____ _____ may point to whether key bits are _____
- Countermeasures may
  - Add _____ plain text
  - Designs with _____ _____ or _____ logic

9.2 Security Attacks Through Fault Injection

- _____ _____ is an important kind of ____-_____ attack.
- _____ _____ techniques
  - Varying the _____ _____
  - Varying the _____ _____
  - Exposing the device to _____ _____
- These techniques affect one or multiple bits or even multiple bytes.
- By analyzing the _____ profile, the vulnerable time of the process is identified.

9.2.1 Fault Attacks on Symmetric Key Ciphers

- In DES devices, the secret key is often kept in _____ and transferred to _____ when needed.
- By setting all bytes but one to zeros and using _____ _____, the attacker can first determine the high order byte.
- Then, move to each byte in _____

DES Key	Output
$K_0 = xx\ xx\ xx\ xx\ xx\ xx\ xx\ xx$	S_0
$K_1 = xx\ xx\ xx\ xx\ xx\ xx\ xx\ 00$	S_1
$K_2 = xx\ xx\ xx\ xx\ xx\ xx\ 00\ 00$	S_2
$K_3 = xx\ xx\ xx\ xx\ xx\ 00\ 00\ 00$	S_3
$K_4 = xx\ xx\ xx\ xx\ 00\ 00\ 00\ 00$	S_4
$K_5 = xx\ xx\ xx\ 00\ 00\ 00\ 00\ 00$	S_5
$K_6 = xx\ xx\ 00\ 00\ 00\ 00\ 00\ 00$	S_6
$K_7 = xx\ 00\ 00\ 00\ 00\ 00\ 00\ 00$	S_7

9.2.2 Fault Attacks on Public (Asymmetric) Key Ciphers

- Unlike symmetric ciphers, only the _____ process may be subject to attacks to determine the secret private key.
- One attack for RSA
  - Given an encrypted message S and its corresponding plaintext M, both _____ to the attacker, the attacker flips a bit of d, producing an _____ _____, M*.

$$\frac{M^*}{M} = \frac{S^{2^i \overline{d_i}}}{S^{2^i d_i}} \bmod N$$

  - Example (e, N) = (7,77) as public key, d=43 (101011) as private key, S = 37, M = 9, M* = 67

9.3 Countermeasures

- A countermeasure must _____ a fault and then prevent the attacker from _____ the _____ of the device after the fault has been _____.
- The output can be _____ (all 0s) or a _____ _____ generated.
- Two approaches
  - _____ the encryption or decryption process.
  - _____ codes
- Trade-off between fault coverage and overhead

9.3.1 Spatial and Temporal Duplication

- _____ duplication requires redundant _____ to allow independent calculations
- _____ redundancy can be applied by using the same _____ _____ or _____ the same software program.
- Recalculation with _____ operands could also be used here.
- Alternative is to have a separate hardware or software unit for executing the _____ procedure (costly for RSA).

9.3.2 Error-Detecting Codes

- First _____ check bits
- For each _____ within encryption _____ check bits
- Periodically compare _____ to _____ check bits
- _____ is the most complex part, complexity of it should be compared to _____

- Examples of EDC – _____ based and _____ checks

- Can be applied at different levels – _____, _____, _____