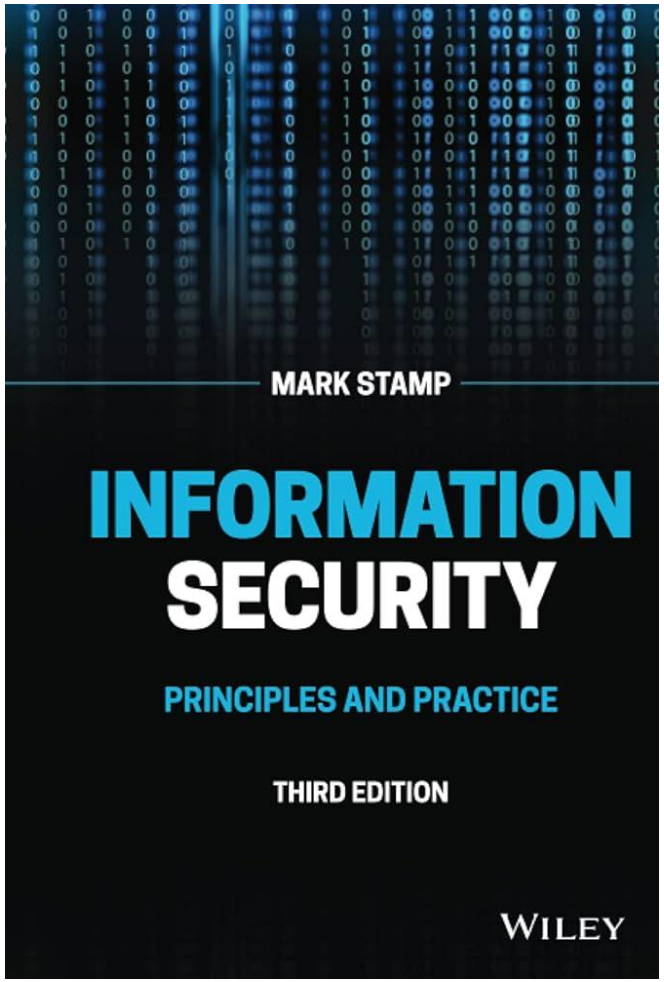
بسم الله الرحمن الرحیم

مبانی رایانش امن

جلسه ۵

مجتبی خلیلی
دانشکده برق و کامپیوتر
دانشگاه صنعتی اصفهان


MARK STAMP
INFORMATION
SECURITY
PRINCIPLES AND PRACTICE
THIRD EDITION
WILEY

- فصل سوم کتاب

Data Encryption Standard(DES)

- DES developed in 1970's
- Based on IBM's Lucifer cipher
- DES was U.S. government standard
- Development of DES was controversial
  - NSA was secretly involved
  - Design process was secret
  - Key length reduced from 128 to 56 bits
  - Subtle changes to Lucifer algorithm

Horst Feistel (1915-1990)

Data Encryption Standard(DES)

- DES is a block cipher with…
  - 64 bit block length
  - 56 bit key length
  - 16 rounds
  - 48 bits of key used each round (subkey)
- Round function is simple (for block cipher)

امنیت DES

- 40+ years of analysis revealed no back door
- Attacks? Essentially exhaustive key search
- **Inescapable conclusions**
  - Designers of DES knew what they were doing
  - Designers of DES were way ahead of their time (at least wrt certain cryptanalytic techniques)

امنیت DES

- همانطور که دیدیم DES دیگر امن نیست.
- خواهیم دید که AES جایگزین آن شده است.
- اما برخی نیز پیشنهاد داده اند که با تغییراتی از DES میتوان استفاده کرد.

درباره DES

$$2DES_{k_1k_2}(m) = DES_{k_2}(DES_{k_1}(m))$$

- با اینکار طول کلید دو برابر میشود.

درباره DES

فرض کنید دشمن m و c را میداند:

$$c = 2DES_{k_1 k_2}(m) = DES_{k_2}(DES_{k_1}(m))$$

$$DES_{k_2}^{-1}(c) = DES_{k_1}(m)$$

k_2

t_1	$DES^{-1}(t_1, c)$
t_N	$DES^{-1}(t_N, c)$

$DES(t_1, m)$	t_1
$DES(t_N, m)$	t_N

k_1

درباره DES

- 56 bit DES key is too small
  - Exhaustive key search is feasible
- But DES was everywhere, so what to do?
- **Triple DES** or **3DES** (112 bit key)
  - $C = E(D(E(P,K_1),K_2),K_1)$
  - $P = D(E(D(C,K_1),K_2),K_1)$
- Why Encrypt-Decrypt-Encrypt with 2 keys?
  - Backward compatible: $E(D(E(P,K),K),K) = E(P,K)$
  - And 112 is a lot of bits

رمزنگاری متقارن (مدرن)

- در حالت کلی رمزنگاری متقارن (مدرن) به دو دسته کلی تقسیم میشوند:

  - الگوریتم‌های رمز جریان (Stream Cipher)

    - ✓ ایده OTP، اما با یک کلید محدود یک کلید بسیار طولانی بسازیم.
    - ✓ مثال: ChaCha20, RC4

  - الگوریتم‌های رمز بلوکی (Block Cipher)

    - ✓ ساخت بلوکهای n بیتی از پیام و رمز آنها با یک الگوریتم تکراری
    - ✓ مثال: AES, DES, 3DES, Blowfish, Twofish

Advanced Encryption Standard(AES)

- NIST در سال ۱۹۹۸: طول کلید ۱۲۸، طول بلاک ۱۲۸، سریعتر

Advanced Encryption Standard(AES)

- Replacement for DES
- AES competition (late 90's)
  - NSA openly involved
  - Transparent selection process
  - Many strong algorithms proposed
  - Rijndael Algorithm ultimately selected (pronounced like "Rain Doll" or "Rhine Doll")
- Iterated block cipher (like DES)
- Not a Feistel cipher (unlike DES)

Advanced Encryption Standard(AES)

- **Block size:** 128 bits (others in Rijndael)
- **Key length:** 128, 192 or 256 bits (independent of block size in Rijndael)
- 10 to 14 rounds (depends on key length)

Advanced Encryption Standard(AES)

- تعداد دور بر اساس کلید:

AES-128: 10 rounds
AES-192: 12 rounds
AES-256: 14 rounds

- تاکنون هیچ حمله موثری به آن نشده است.

Block Cipher Modes

Multiple Blocks

- How to encrypt multiple blocks?
- Do we need a new key for each block?
  - If so, as impractical as a one-time pad!
- Encrypt each block independently?
- How to handle partial blocks?
  - We won't discuss this issue

ECB Mode

- Notation: $C = E(P, K)$
- Given plaintext $P_0, P_1, \ldots, P_m, \ldots$
- Most obvious way to use a block cipher:

Encrypt	Decrypt
$C_0 = E(P_0, K)$	$P_0 = D(C_0, K)$
$C_1 = E(P_1, K)$	$P_1 = D(C_1, K)$
$C_2 = E(P_2, K) \ \ldots$	$P_2 = D(C_2, K) \ \ldots$

ECB Cut and Paste

- Suppose plaintext is

  `Alice digs Bob. Trudy digs Tom.`

- Assuming 64-bit blocks and 8-bit *ASCII*:

  P_0 = "`Alice di`", P_1 = "`gs Bob. `",

  P_2 = "`Trudy di`", P_3 = "`gs Tom. `"

- Ciphertext: C_0, C_1, C_2, C_3
- Trudy cuts and pastes: C_0, C_3, C_2, C_1
- Decrypts as

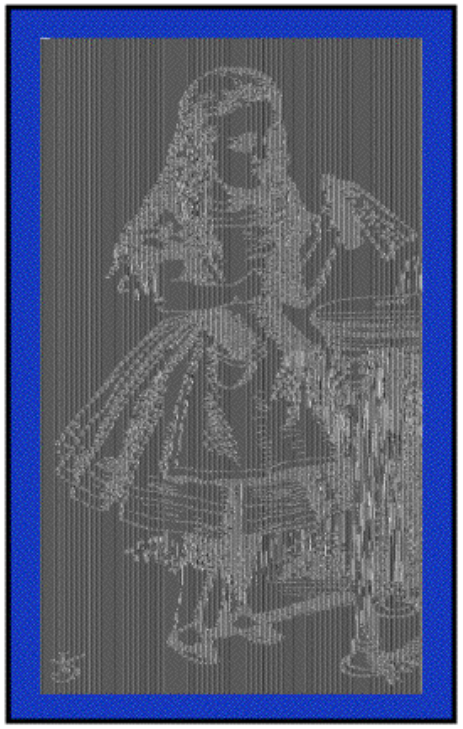
  `Alice digs Tom. Trudy digs Bob.`

ECB Weakness

- Suppose $P_i = P_j$
- Then $C_i = C_j$ and Trudy knows $P_i = P_j$
- This gives Trudy some information, even if she does not know P_i or P_j
- Trudy might know P_i
- Is this a serious issue?

Alice Hates ECB Mode

- Alice's uncompressed image, and ECB encrypted



- Why does this happen?
- Same plaintext yields same ciphertext!