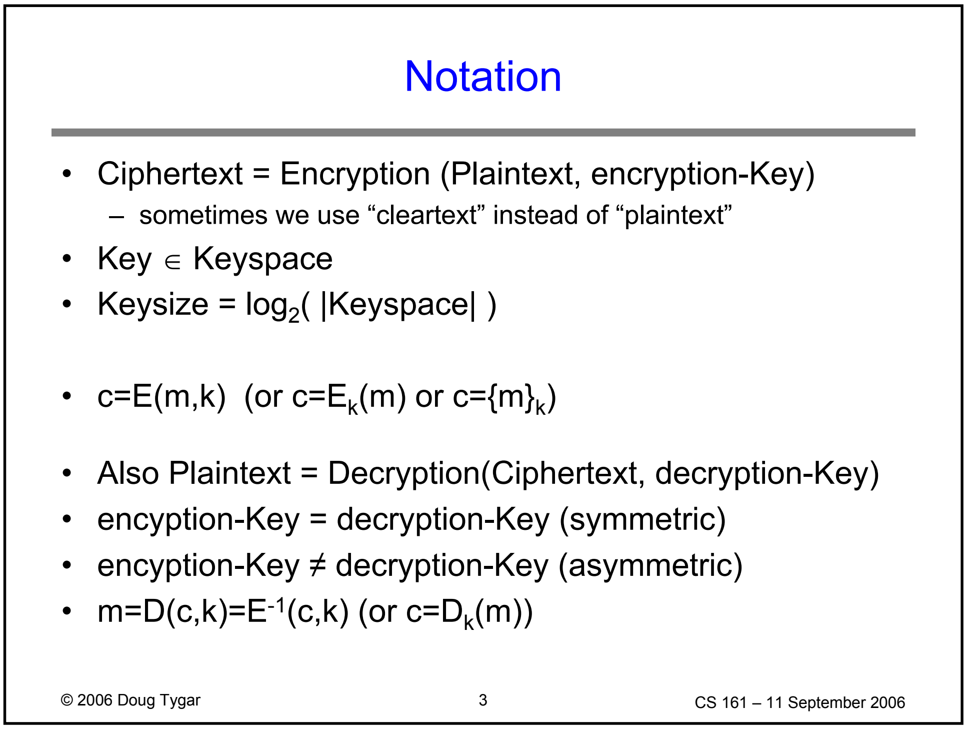
CS 161 – Introduction to Cryptography; Symmetric Cryptography

11 September 2006

Cryptography

- History: Gallic Wars to WW2 (Enigma, Purple)
- Ciphers vs. codes
- Cryptology
  - Cryptography: making ciphers
  - Cryptanalysis: breaking ciphers
  - Traffic analysis: watching patterns of communications
- Need: communications can be tapped
- Building block for cryptographic protocols

- In the US: National Security Agency

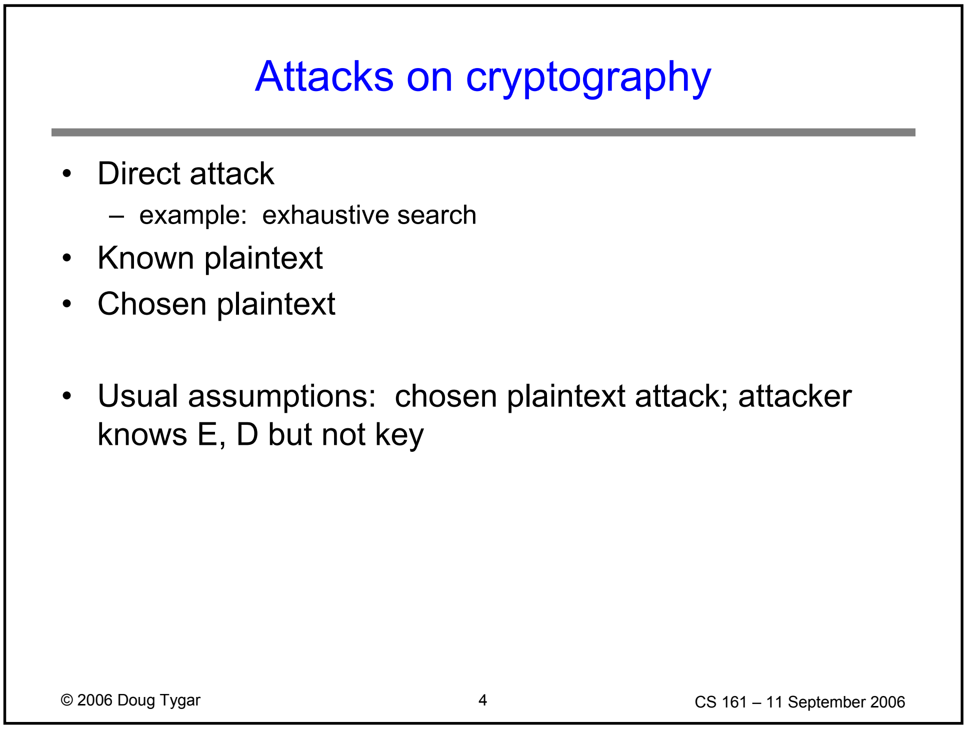


Notation

- Ciphertext = Encryption (Plaintext, encryption-Key)
  - sometimes we use “cleartext” instead of “plaintext”
- Key $\in$ Keyspace
- Keysize = $\log_2$(|Keyspace|)

- $c=E(m,k)$ (or $c=E_k(m)$ or $c=\{m\}_k$)

- Also Plaintext = Decryption(Ciphertext, decryption-Key)
- encyption-Key = decryption-Key (symmetric)
- encyption-Key ≠ decryption-Key (asymmetric)
- $m=D(c,k)=E^{-1}(c,k)$ (or $c=D_k(m)$)



Attacks on cryptography

- Direct attack
  - example: exhaustive search
- Known plaintext
- Chosen plaintext

- Usual assumptions: chosen plaintext attack; attacker knows E, D but not key

Perfect cryptosystem

- One-time pad
- Share a common key (key size ≥ message size)
- XOR key with message

- No information at all is leaked
  - Why?

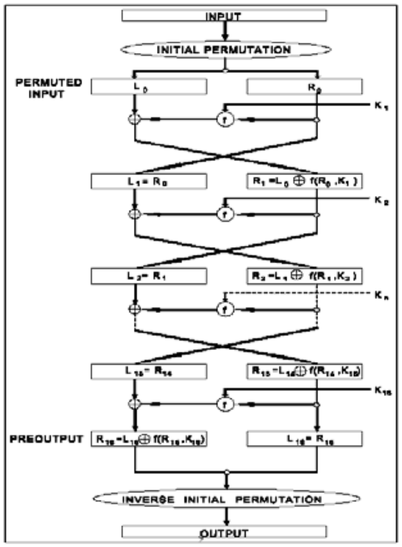
- What problem does this system have?

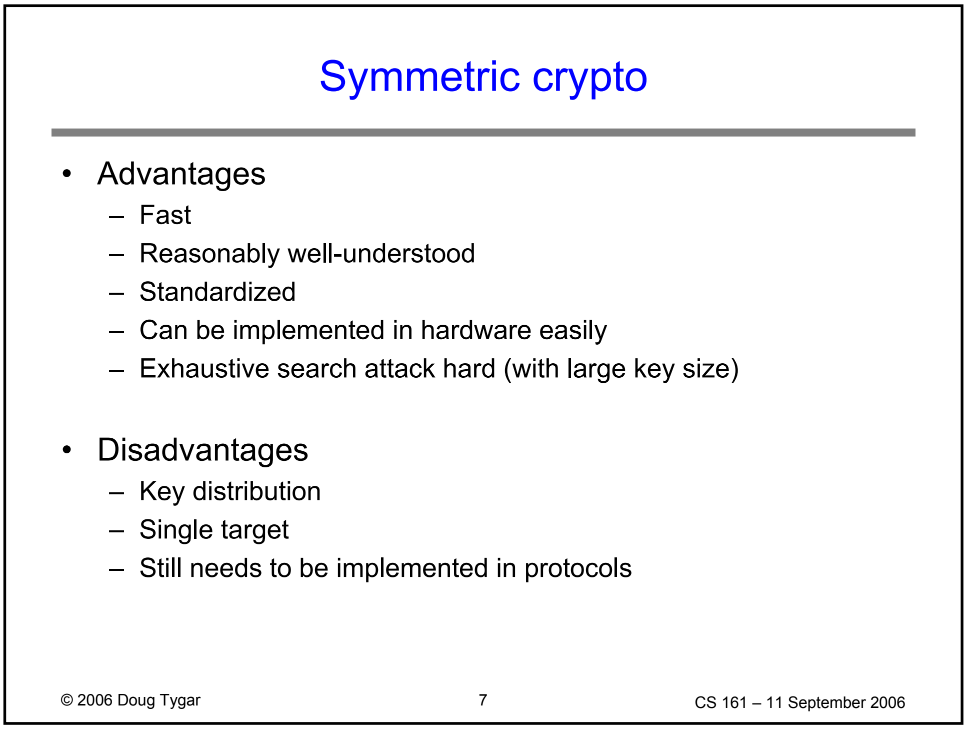
DES

- Origins: mid-70s
- History: (Lucifer, NIST, NSA)
- 56 bit key, 64 bit block cipher

- Differential cryptanalysis
- Exhaustive search

- AES (Rijndael)
- 128-256 bit key, 128 bit block cipher


INPUT
INITIAL PERMUTATION
PERMUTED INPUT
L_0
R_0
K_1
f
$L_1 = R_0$
$R_1 = L_0 \oplus f(R_0, K_1)$
K_2
f
$L_2 = R_1$
$R_2 = L_1 \oplus f(R_1, K_2)$
K_n
f
$L_{15} = R_{14}$
$R_{15} = L_{14} \oplus f(R_{14}, K_{15})$
K_{16}
f
PREOUTPUT
$R_{16} = L_{15} \oplus f(R_{15}, K_{16})$
$L_{16} = R_{15}$
INVERSE INITIAL PERMUTATION
OUTPUT



Symmetric crypto

- Advantages
  - Fast
  - Reasonably well-understood
  - Standardized
  - Can be implemented in hardware easily
  - Exhaustive search attack hard (with large key size)
- Disadvantages
  - Key distribution
  - Single target
  - Still needs to be implemented in protocols