Cryptography & Attacking crypto

Lecture 5 - ECS198F SQ26

Agenda

- DES
- AES

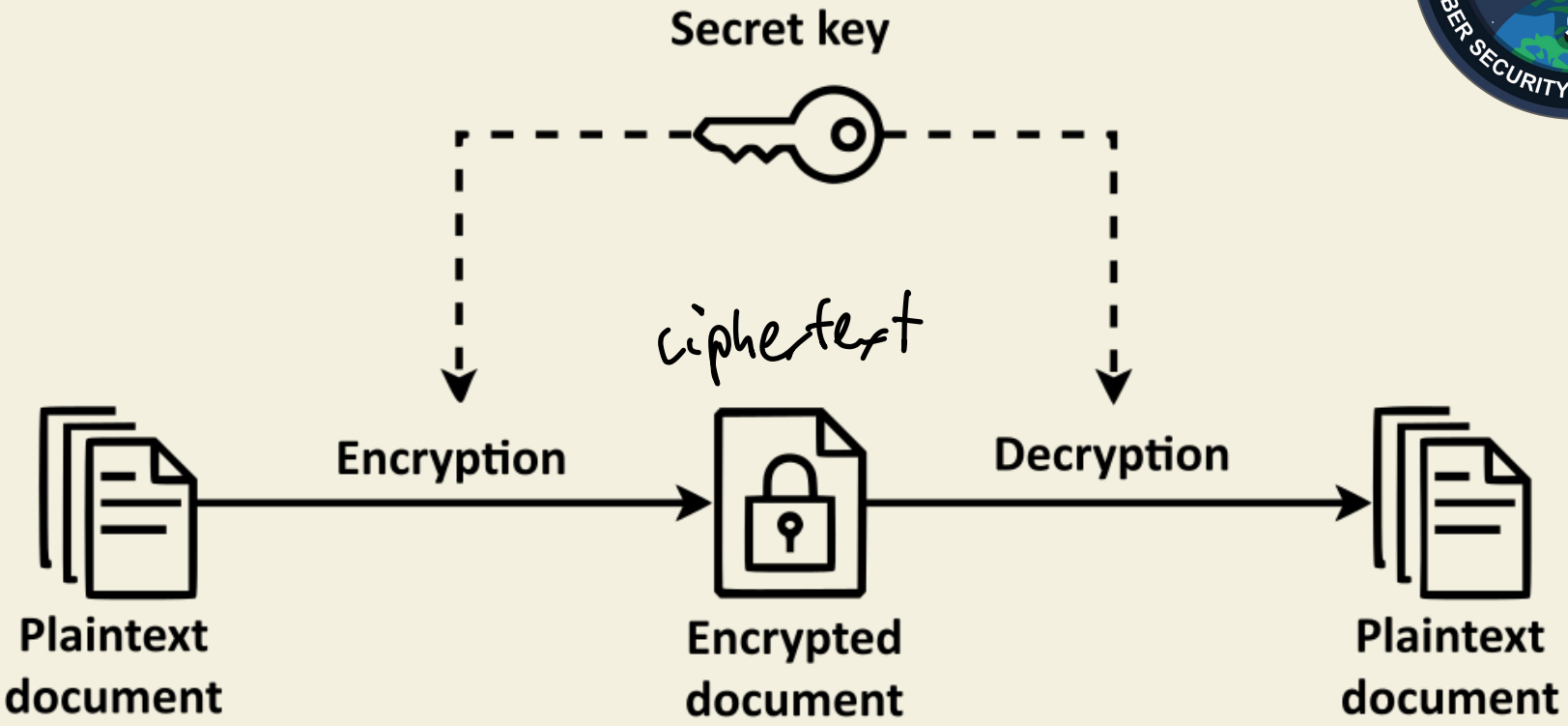
} Symmetric algo

- DH
- RSA

} Asymmetric algo

- Attacks!!

Symmetric Algorithms



One time pad

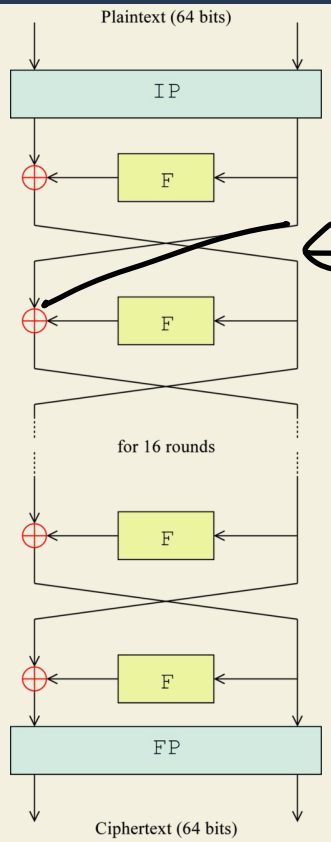
key length == plaintext

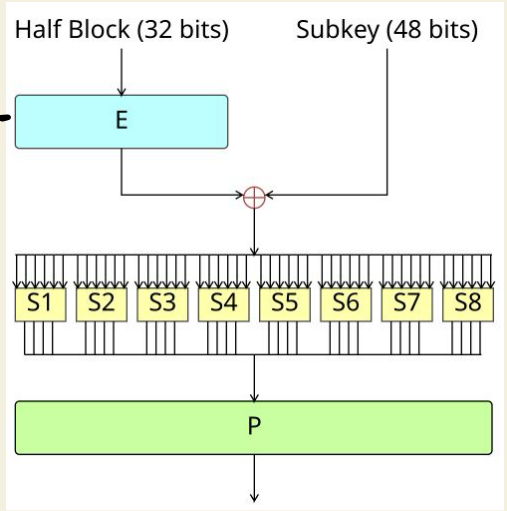
key random

key never unused

key is secret

Data Encryption Standard





64 bits ⇒ 56 bits

2^{56}

XOR = mod 2

bit$_0$	bit$_1$	add
0	0	0
0	1	1
1	0	1
1	1	0

DES

Claude Shannon :

Diffusion

Confusion

DES

Differential Cryptanalysis (T-attack)

↳ chosen plaintext & ciphertext

Linear

↳ known

DES

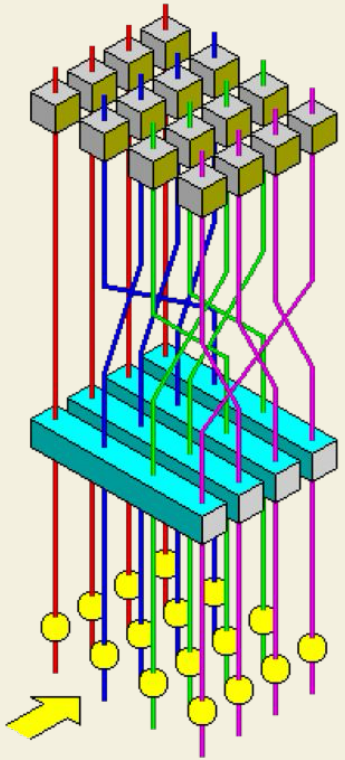

$C_1 \Leftrightarrow P_2$
C_2
2^{56}
2^{56}
P_1
DES
DES
DES
C
56 bit + 56 bit = 57 bit + 56 bits
Meet in the middle Attack
3DES
113
2

2 ways of attacking crypto

- Inherent structure
- Key length

side channel attacks

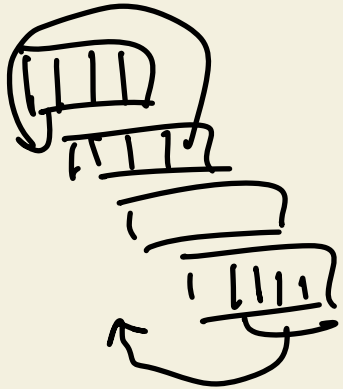
Advanced Encryption Standard



P

GF(2^8)

← S boxes



← XOR

C

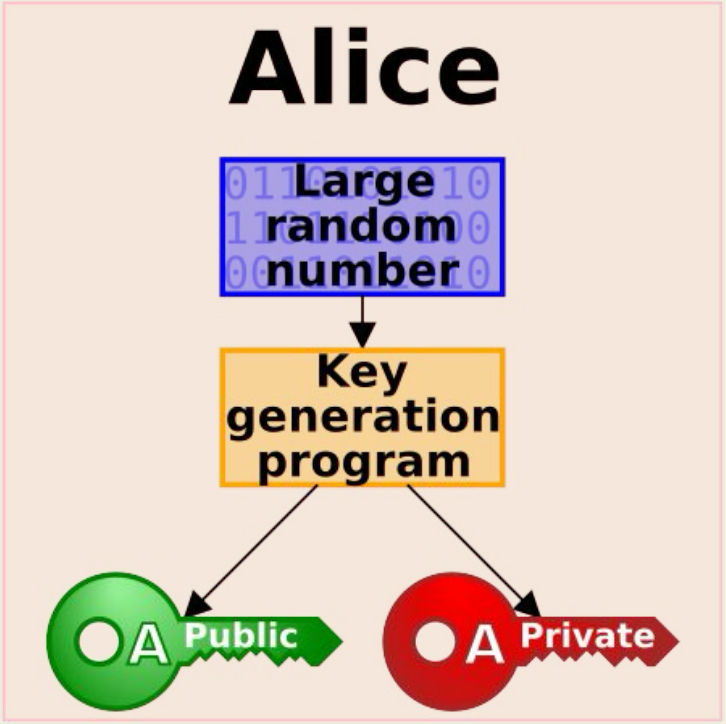
10 / 12 / 14

128 192 256

$A \oplus K \oplus K = A$

AES

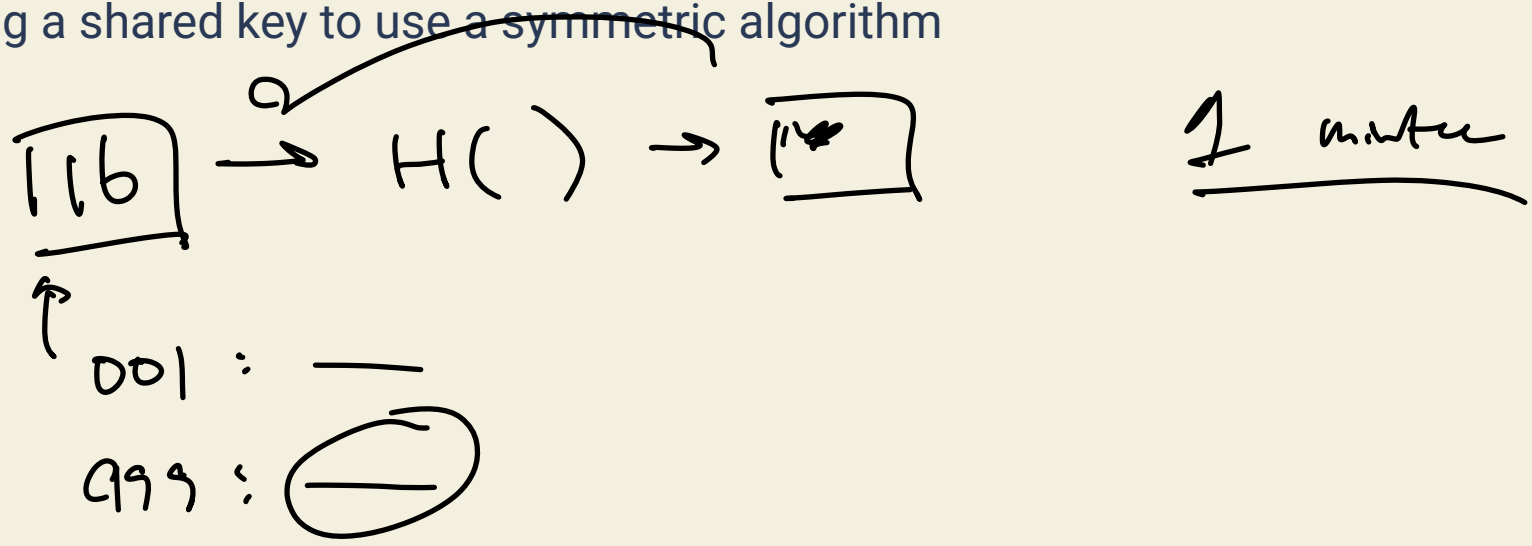
Asymmetric Algorithms



Merkle's Puzzle

Problem:

Getting a shared key to use a ~~symmetric~~ algorithm



Diffie Hellman

Eve

(g, p)

(g, p, g^a) Alice's pub

priv Alice

$a = \{2..p-1\}$

$g^a \bmod p = A$

$B^a = (g^b)^a$

$= g^{ab}$

$A \; g^a \rightarrow$

$\leftarrow B \; g^b$

$g^a \cdot g^b = g^{a+b}$

Bob

$b = \{2..p-1\}$

$g^b \bmod p = B$

$A^b = (g^a)^b$

$= g^{ab}$

Diffie Hellman

Discrete Log

$$y = a^x \bmod p$$

primitive root

$x \leftarrow y, a, p$ (a generator of p)

$g^{\{2..p-1\}} \Rightarrow$

Diffie Hellman

$k = r^a \mod p$ (r, p, k)

$M = (r^k, MK^k)$ K random

$(r^k)^a \cdot MK^k = M \mod p$

El Gamal (DSA)

RSA

$n = pq$ $\quad e = (e, \phi(n)) = 1$ ← pub

$C = M^e \bmod n \quad (n, e)$

$M = C^d \bmod n \leftarrow ed \equiv 1 \bmod \phi(n)$ ← priv

$\phi(n) = (p-1)(q-1)$

$S = M^d \bmod n$

$V(S) = S^e \bmod n$

$(M^d)^e = M^{de} = M$

Table 2: Comparable security strengths of symmetric block cipher and asymmetric-key algorithms

Security Strength	Symmetric Key Algorithms	FFC (DSA, DH, MQV)	IFC* (RSA)	ECC* (ECDSA, EdDSA, DH, MQV)
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

* The security-strength estimates will be significantly affected when quantum computing becomes a practical consideration.

Grover's

Shor's

$\mathbb{Z}_{2^{256}}$

g^a

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

published in 2020

Takeaways?

Very Important :

DON'T ROLL

YOUR OWN CRYPTO.

* unless you have multiple advanced math / cs degrees or you work for {FBI, CIA, NSA} ...