Cryptography & Attacking crypto

Lecture 5 - ECS198F SQ26

Agenda

- DES
- AES

} Symmetric algo

- DH
- RSA

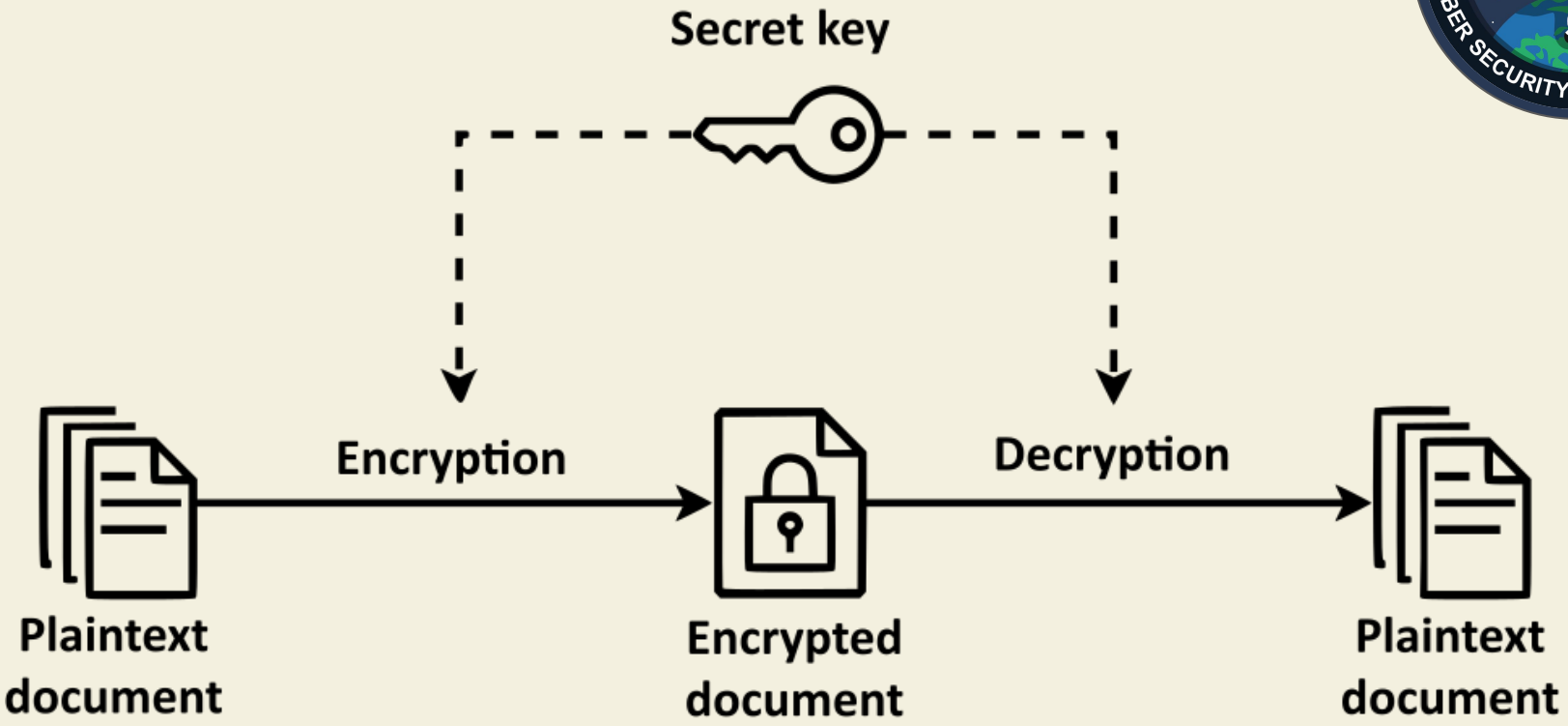
} Asymmetric algo

- Attacks!!

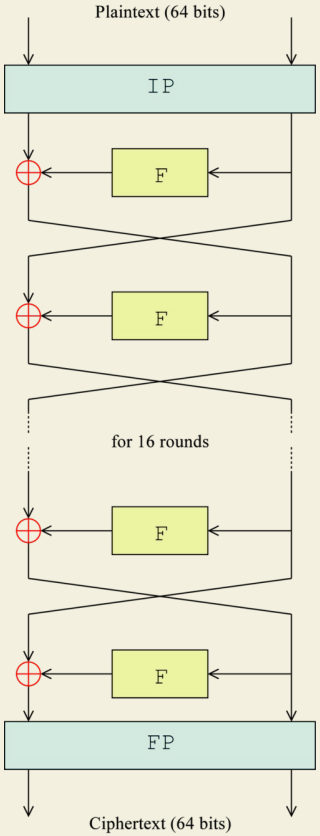
2 ways of attacking crypto

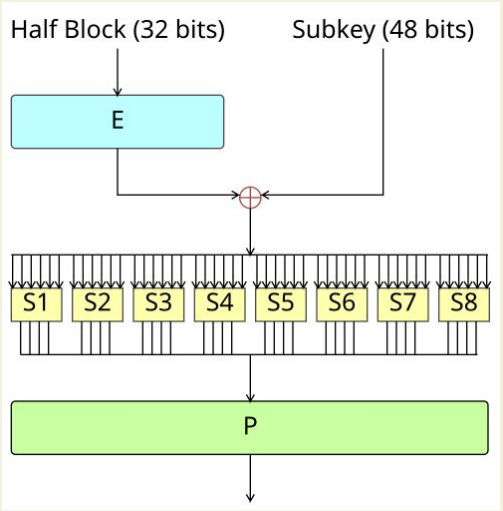
- Inherent structure
- Key length

Symmetric Algorithms



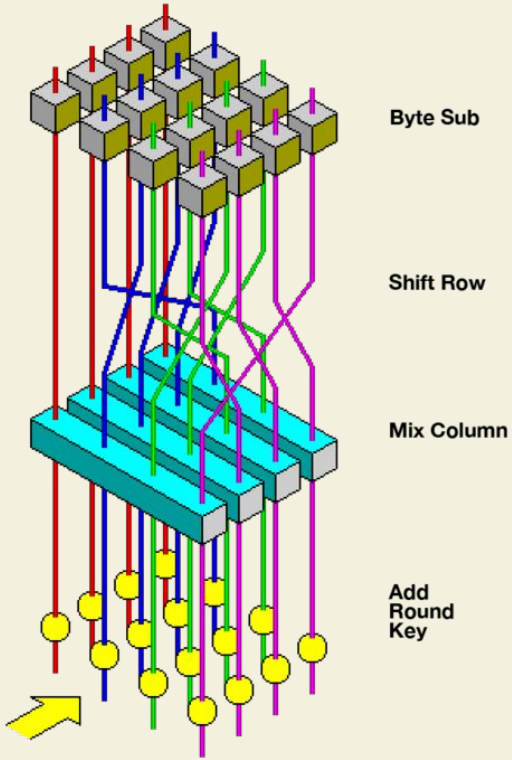
Data Encryption Standard





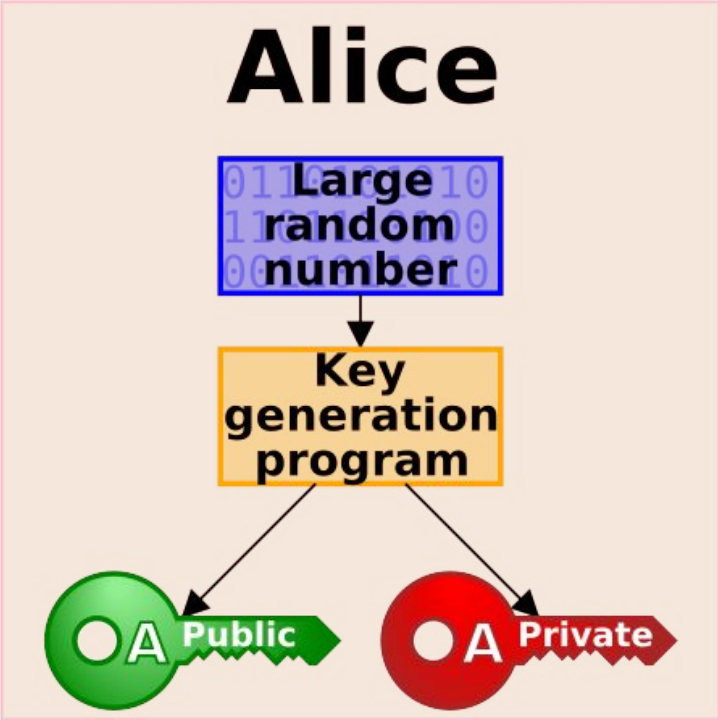
DES

Advanced Encryption Standard



AES

Asymmetric Algorithms



Merkle's Puzzle

Problem:

Getting a shared key to use a symmetric algorithm

Diffie Hellman

RSA


CYBER SECURITY CLUB AT UC DAVIS

Takeaways?


CYBER SECURITY CLUB AT UC DAVIS