Data & Network Security

Applied!

Behnam Amiri

ans.dailysec.ir

aNetSec.github.io

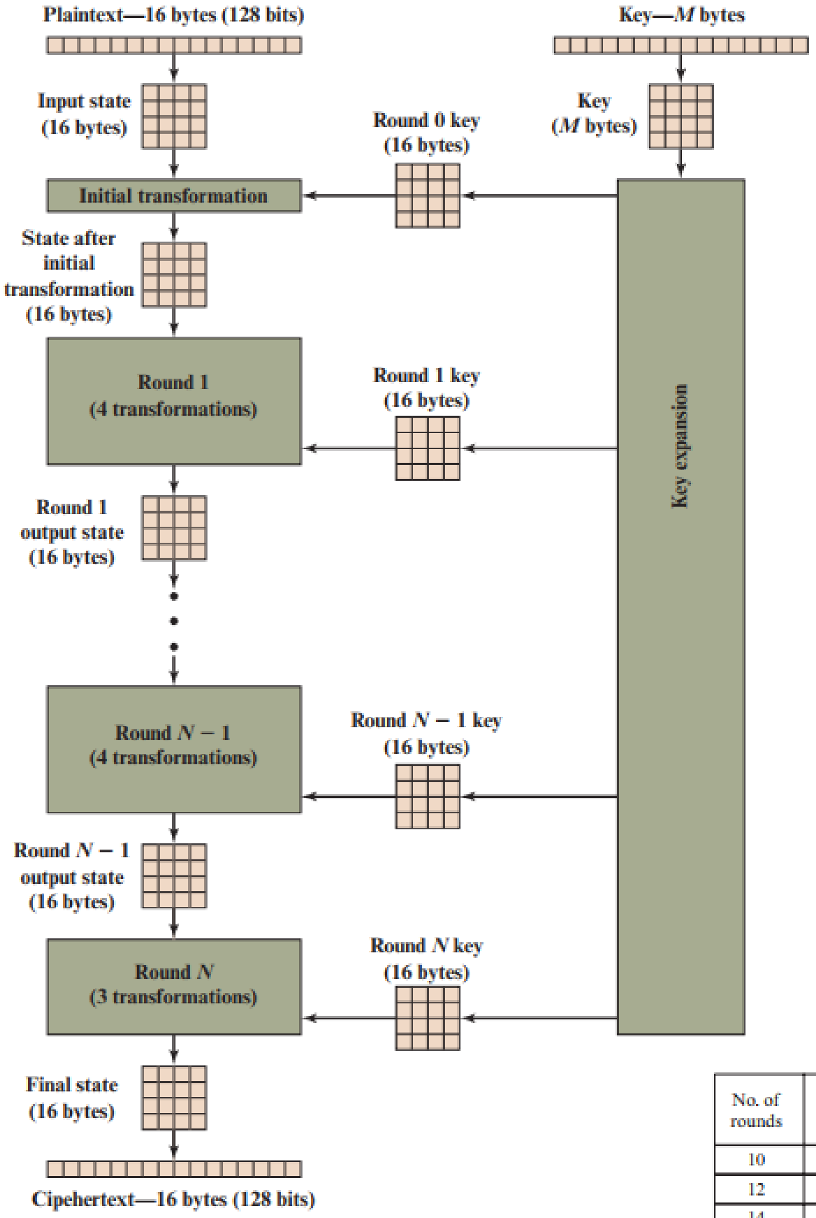
Spring 2025

Modern Cryptography

Advanced Encryption Standard (AES)

- In 1997 NIST- National Institute of Standards and Technology start competition.
- Submited designs: CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, Rijndael, SAFER+, Serpent, and Twofish.
- In 2000, NIST announced that Rijndael had been selected.
- AES Published by the NIST in 2001
- AES is a symmetric block cipher

AES

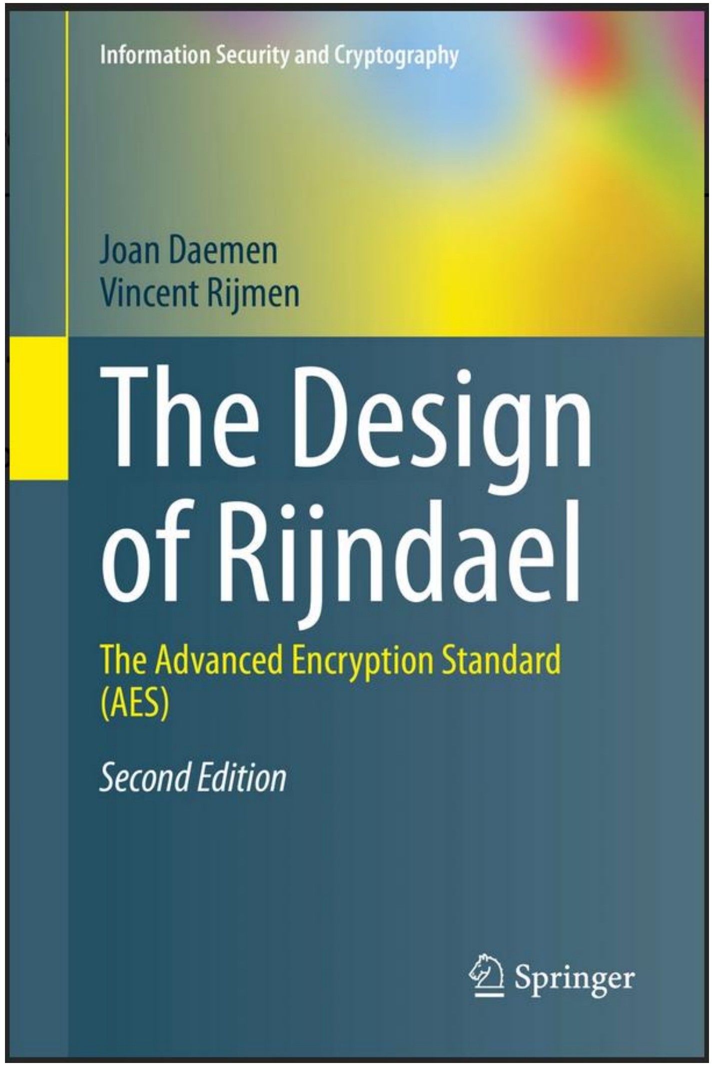


No. of rounds	Key Length (bytes)
10	16
12	24
14	32

Figure 6.1 AES Encryption Process

AES

- The Design of Rijndael book
  - Joan Daemen
  - Vincent Rijmen



Why AES is transparent?

- Kerckhoffs's principle
  - cryptosystem should be secure, even if everything about the system, except the key, is public knowledge.

$\neq$

- Security through obscurity
  - is concealing the details or mechanisms of a system to enhance its security

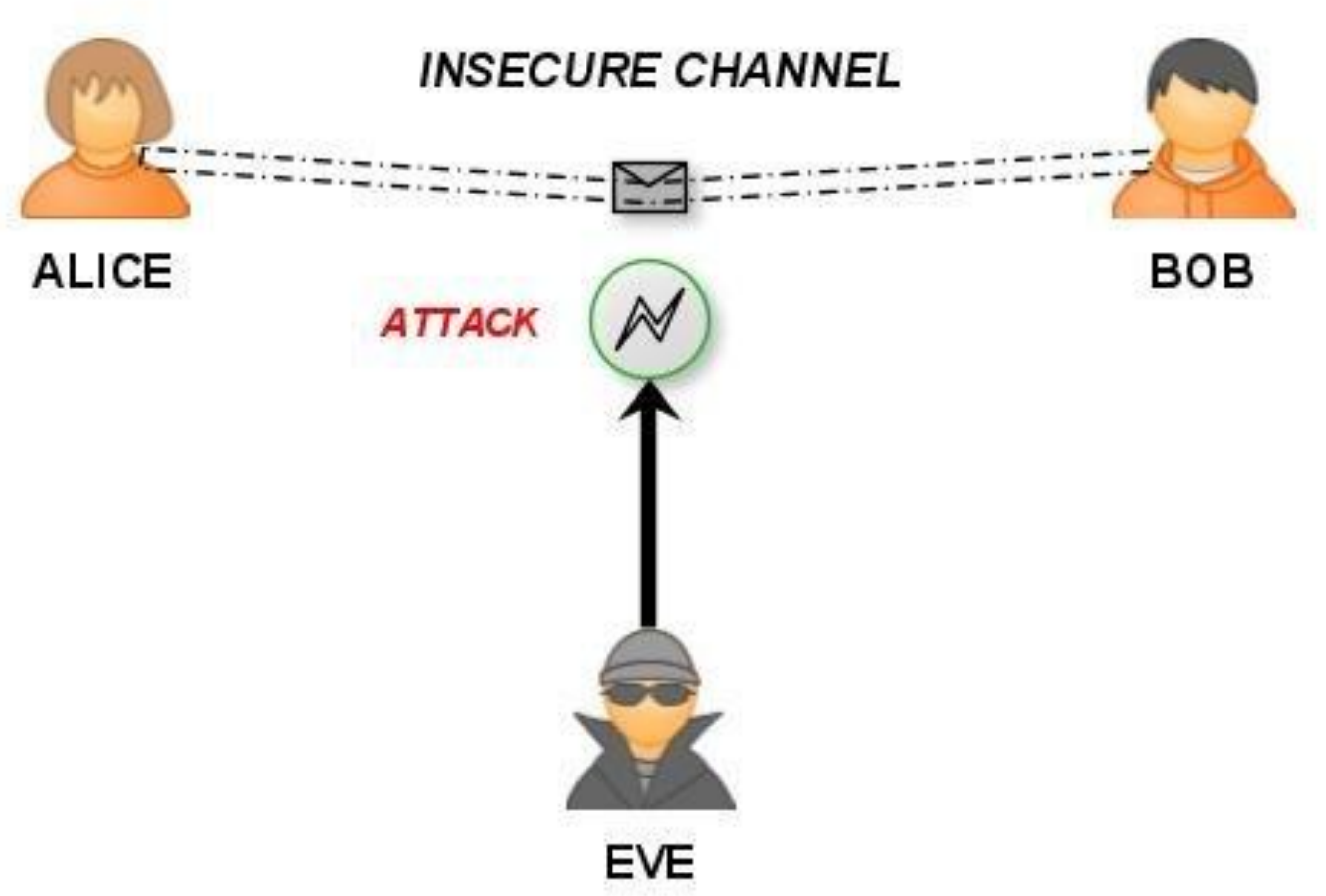
Why AES is transparent?

AES

Key Size	Number of Possible Keys	Assumptions	Encryption/Decryption Time
AES-128	2^128≈3.4×1038	Assuming 1 billion keys tested per second, it would take about 10^21 years.	Fast
AES-192	2^192≈6.3×1057	Same assumption as above.	Medium
AES-256	2^256≈1.1×1077	Same assumption as above.	Slow

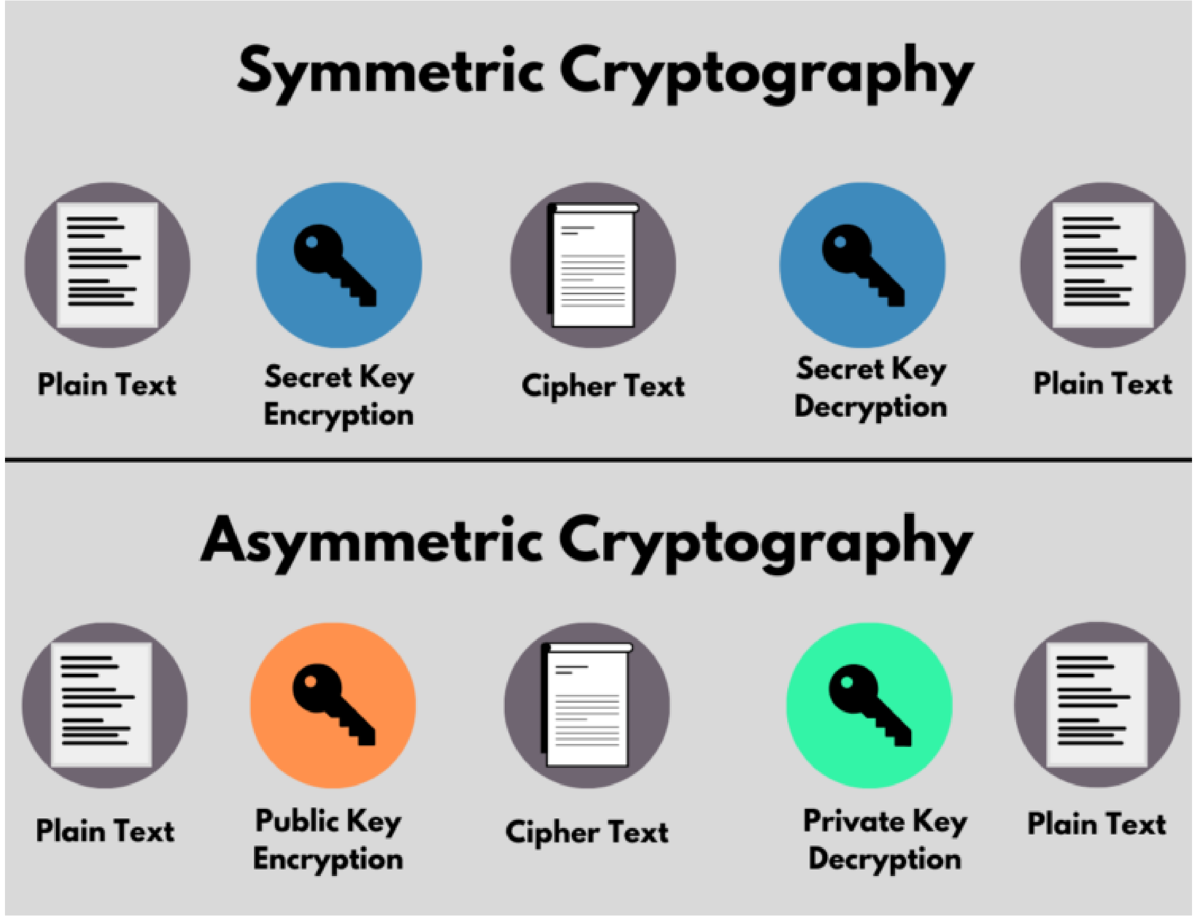
- Postquantum computers can break it faster!
- We should use postquantum algorithms?!

Bob & Alice!



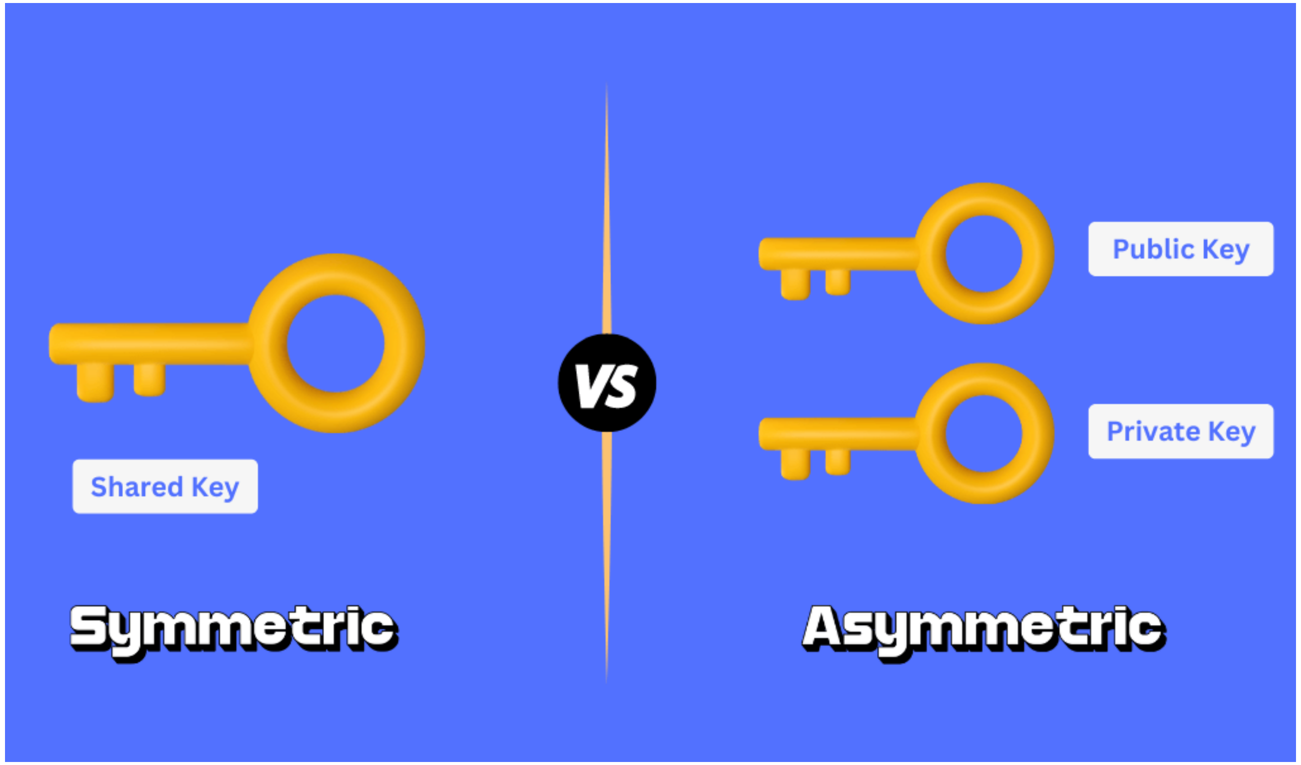
Symmetric vs Asymmetric Encryption

- Symmetric
  - Same key for encryption & decryption
- Asymmetric
  - Different Keys for encryption & decryption

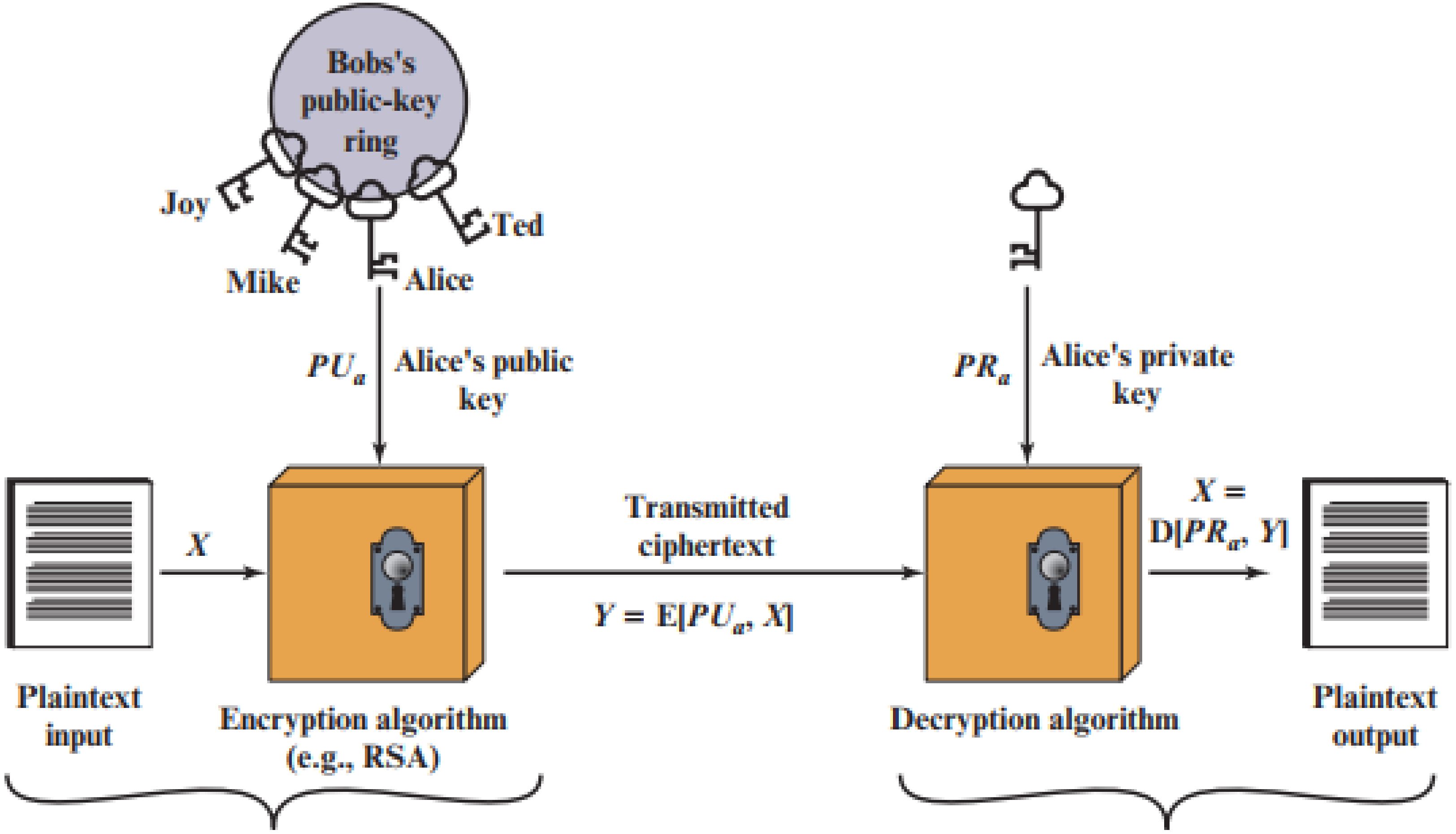


Public & Private Key

- Public Key
  - Used for encryption
  - Is public
  - Shared
- Private Key
  - Used for decryption
  - Is private
  - Not shared
- PU_a is public key of person A
- PR_a is private key of person A

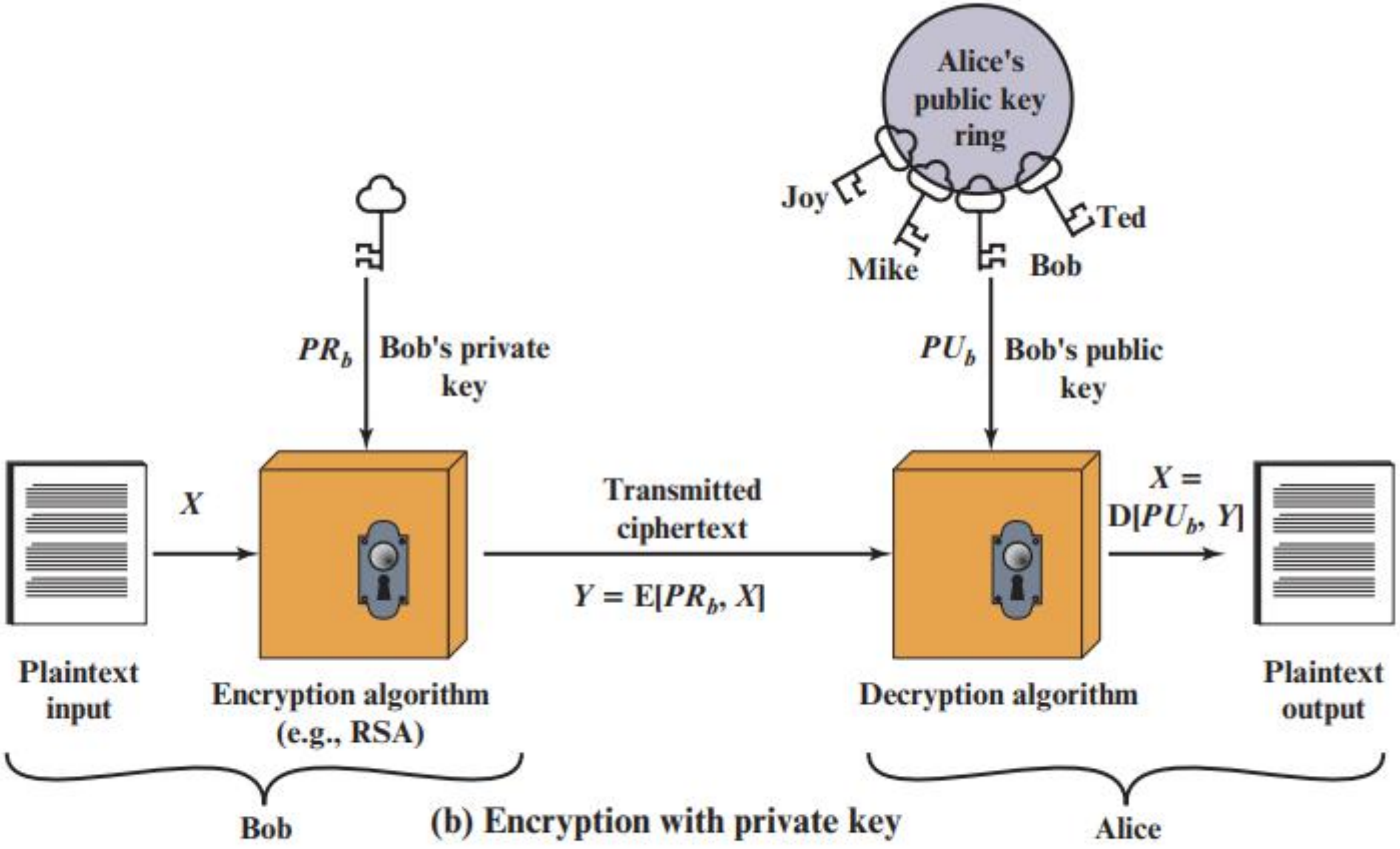


Encryption with public key



(a) Encryption with public key

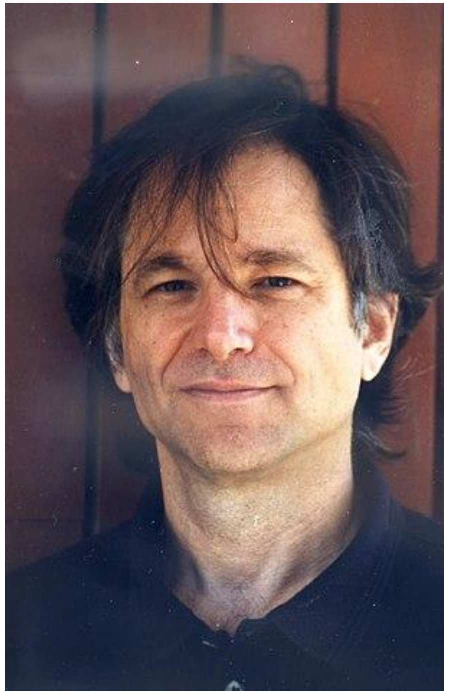
Encryption with private key – not common



(b) Encryption with private key

RSA

- RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem
- publicly described in 1977 in MIT



How it works?

Key Generation by Alice

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

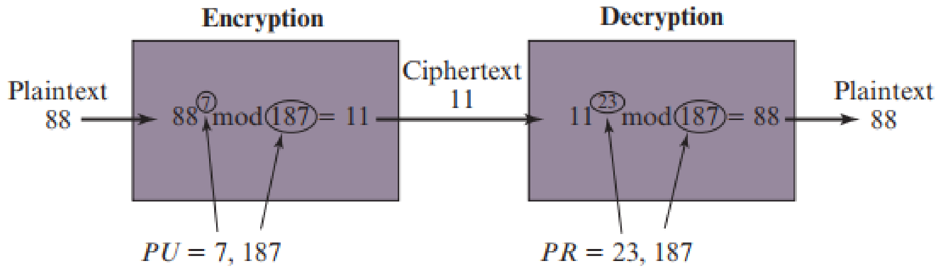
Encryption by Bob with Alice's Public Key

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Private Key

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Figure 9.5 The RSA Algorithm

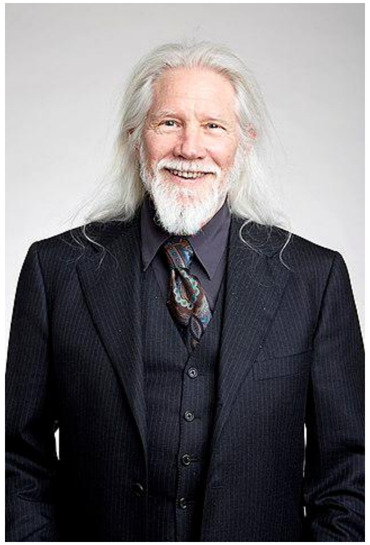


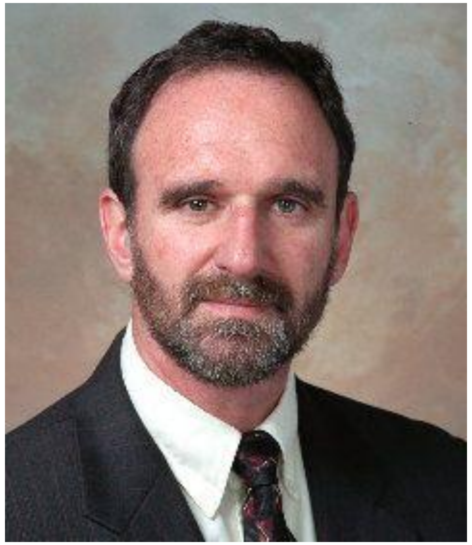
Compare

Feature	Symmetric	Asymmetric
Encryption	Session Key	Public key
Decryption	Session Key	Private key
Speed	Faster	Slower
Key exchange challenge	Yes	No
Message Length	No limit	Limited to key length
Common Algorithms	3DES,AES, CAST, Two Fish, Blowfish, ChaCha20	RSA, El Gamal, DSA, ECDSA

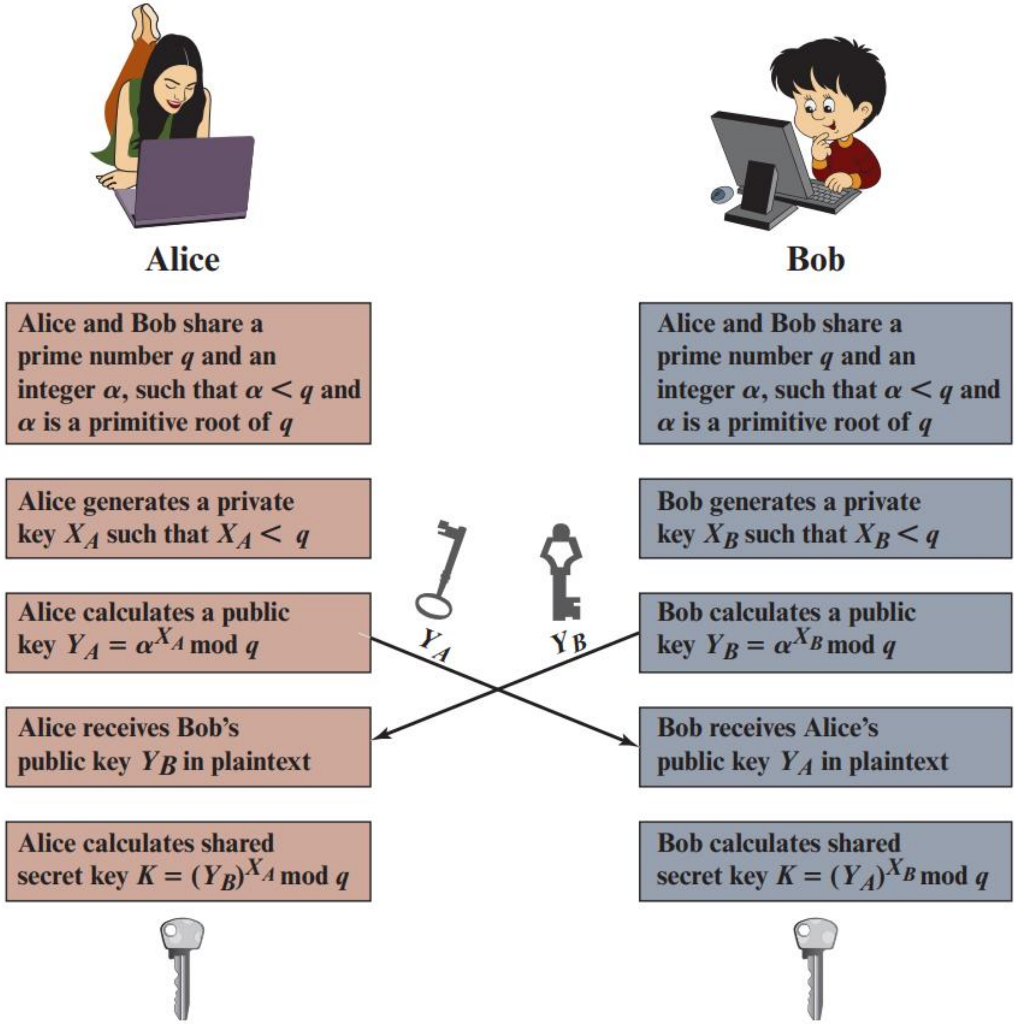
Diffie–Hellman Key Exchange

- The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages.
- The scheme was published by Whitfield Diffie and Martin Hellman in 1976.

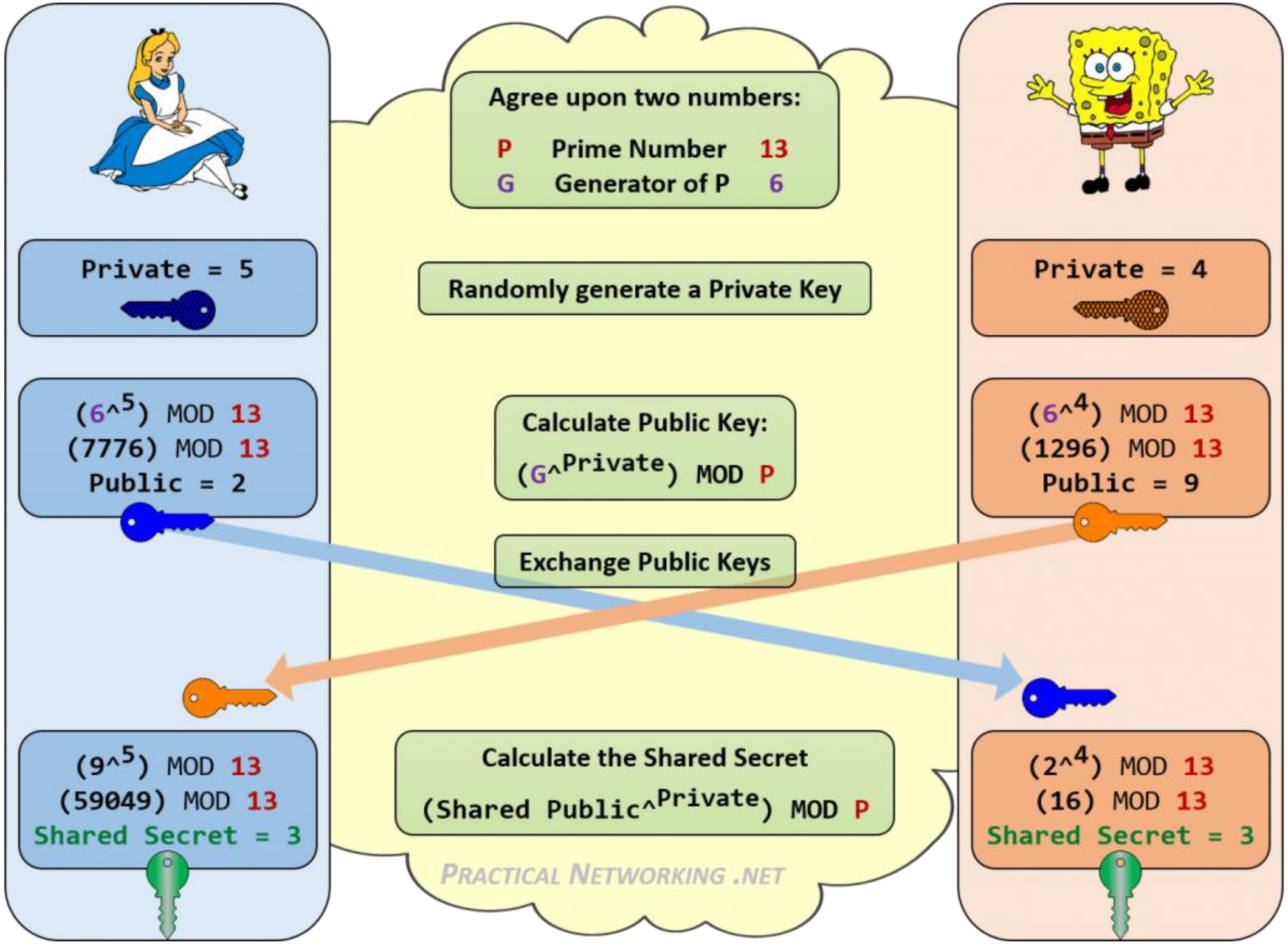




Diffie–Hellman Key Exchange



Diffie–Hellman Key Exchange



Forward Secrecy

- Forward Secrecy (FS), also known as perfect forward secrecy (PFS)
- is a feature of specific key-agreement protocols that gives assurances that session keys are different!

No Forward Secrecy

Day 1

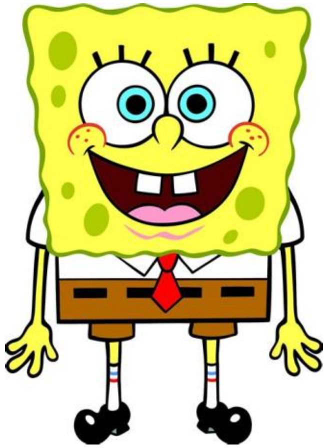
Encrypted Data with key

Day 2

Encrypted Data with key

Day 3

Encrypted Data with key



Find Key!

Can read previous days data

Forward Secrecy

Day 1

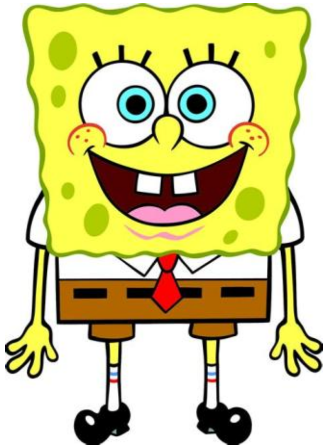
Encrypted Data with key Day 1

Day 2

Encrypted Data with key Day 2

Day 3

Encrypted Data with key Day 3

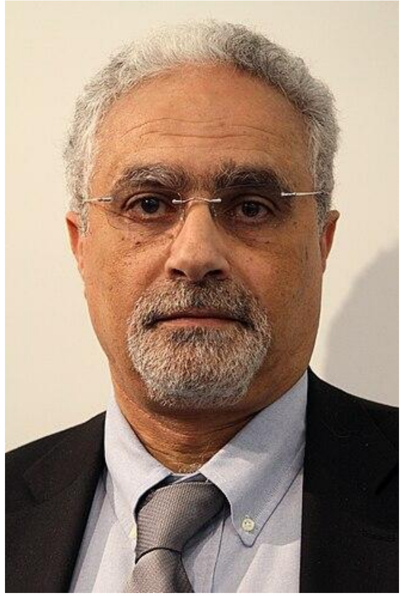


Find Key Day3

Just can read Day3 data!

ElGamal encryption

- ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange.
- ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP.
- It was described by Taher El-Gamal in 1985.



Compare

Feature	RSA	Diffie-Hellman	ElGamal
Type	Asymmetric encryption	Key exchange	Asymmetric encryption
Key Generation	Based on two large primes	Based on a large prime and generator	Based on a large prime and generator
Use Case	Secure data transmission, digital signatures	Secure key exchange	Secure data transmission, digital signatures
Security Basis	Difficulty of factoring large composite numbers	Difficulty of discrete logarithm problem	Difficulty of discrete logarithm problem
Performance	Slower; used for small data or key encryption	Generally faster for key exchange	Slower than RSA for encryption; larger ciphertext
Key Size	Commonly 2048 bits or more	Commonly 2048 bits or more	Commonly 2048 bits or more
Main Disadvantage	Slower performance, larger key sizes	Only for key exchange, not encryption	Slower performance, larger ciphertext

Public Key Usages

- Encryption
- Digital sign
- Key Distribution