

Cryptography Primer

CS-576 Systems Security

Instructor: Georgios Portokalidis

Fall 2018

Goals of Cryptography

Confidentiality

- Keep content secret from unauthorized entities

Integrity

- Protect content from unauthorized modification

Authentication

- Confirm the identity of communicating entities
- Confirm the identify of data author

Non-repudiation

- Prevent entities from denying previous commitments or actions

Overview

Symmetric encryption

Public-key encryption

Hashing and message authentication codes

Symmetric Encryption

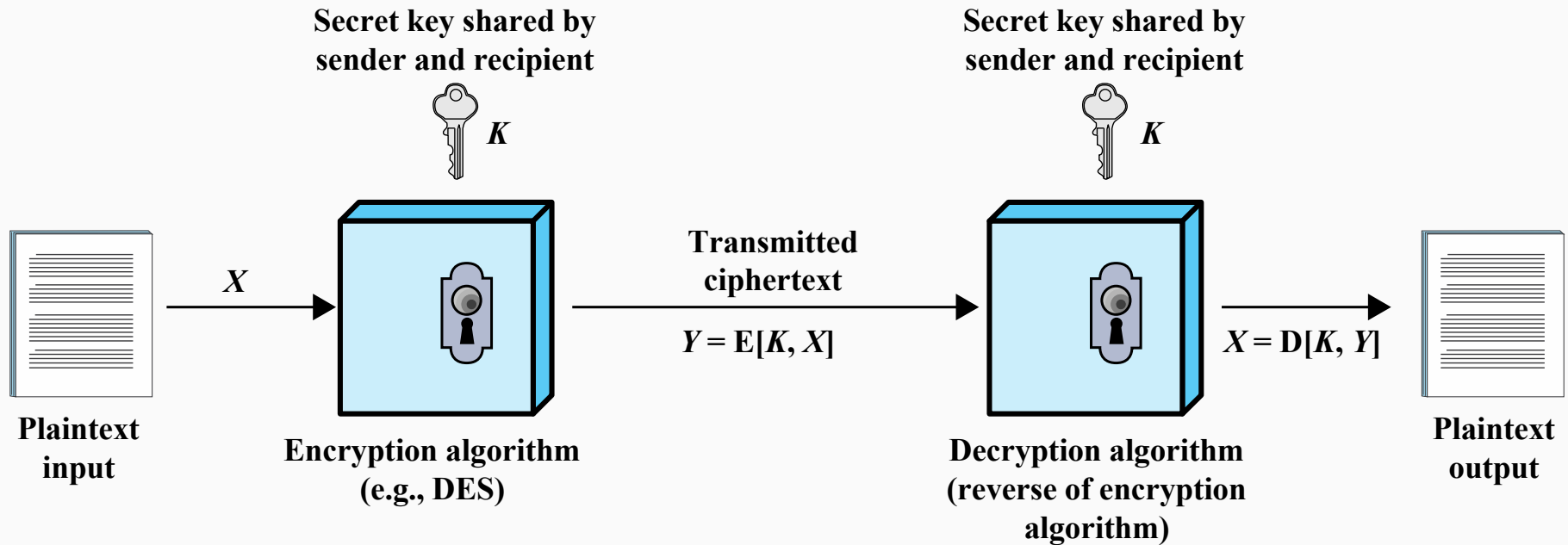
The universal technique for providing confidentiality for transmitted or stored data

Also referred to as conventional encryption or single-key/secret-key encryption

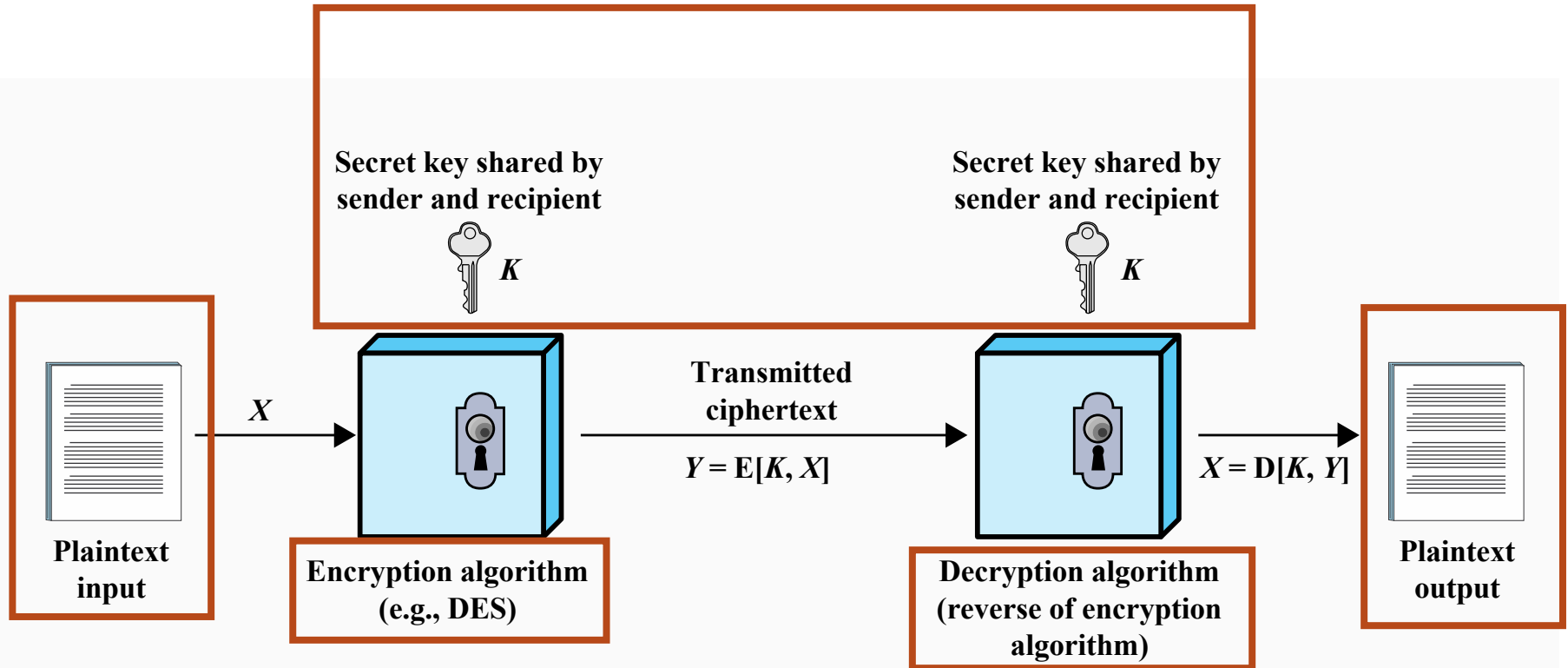
Two requirements for secure use:

- A strong encryption algorithm
- Sender and receiver **must have obtained copies of the secret key in a secure fashion** and **must keep the key secure**

Overview



Terminology



Types of Ciphers

Block ciphers

Processes the input one block of elements at a time

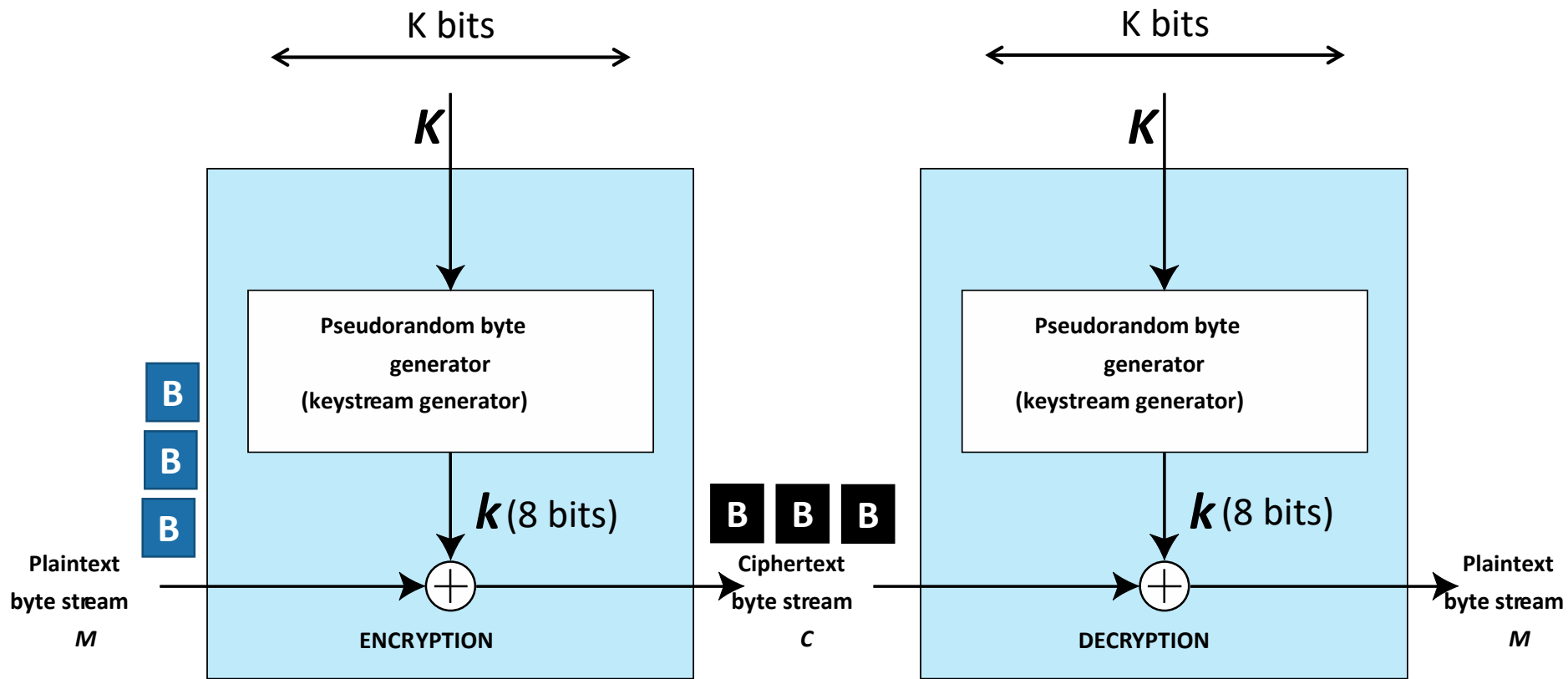
Produces an output block for each input block

Stream ciphers

Processes the input and produces output one element at a time

Requires unpredictable pseudorandom stream independent of the key

Stream Ciphers



Beware of Randomness

Cryptographic algorithms frequently require random numbers

A true random number generator (TRNG)

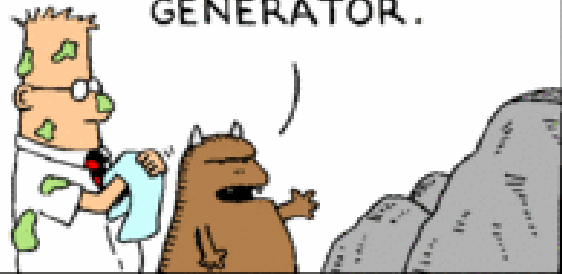
- Uses a nondeterministic source to produce randomness
- Most operate by measuring unpredictable natural processes
 - e.g., radiation, gas discharge, leaky capacitors
- Available on modern systems, but cannot provide high-volume of data

Pseudorandom numbers are

- Sequences produced that satisfy statistical randomness tests
- Likely to be predictable
- **Likely to be used by implementations**

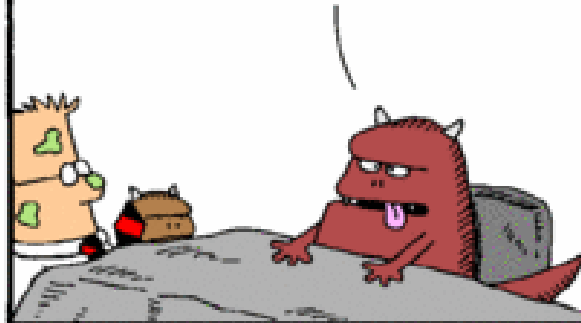
TOUR OF ACCOUNTING

OVER HERE
WE HAVE OUR
RANDOM NUMBER
GENERATOR.



www.dilbert.com
scottadams@aol.com

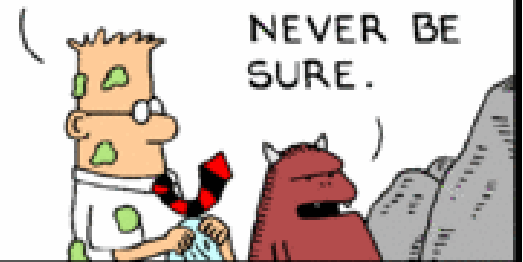
NINE NINE
NINE NINE
NINE NINE



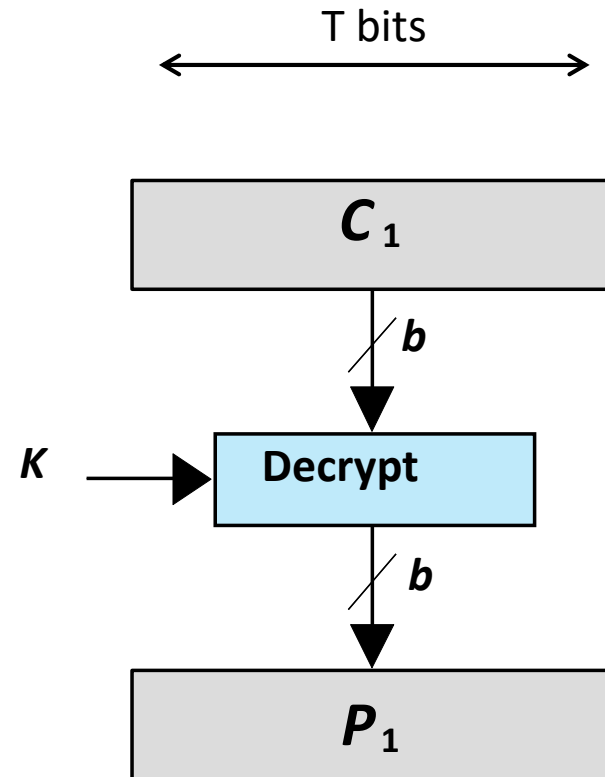
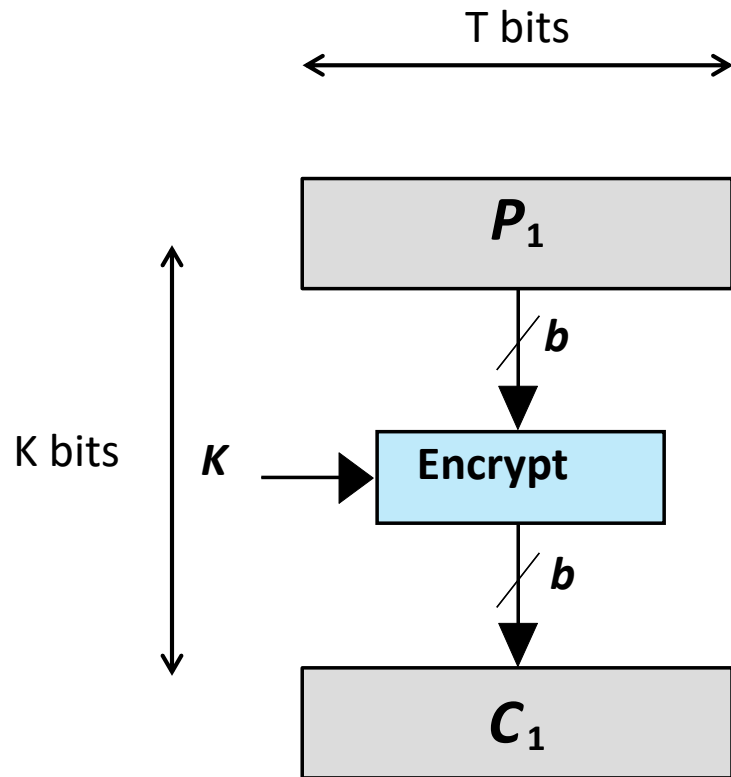
© 2001 United Feature Syndicate, Inc.

ARE
YOU
SURE
THAT'S
RANDOM?

THAT'S THE
PROBLEM
WITH RAN-
DOMNESS:
YOU CAN
NEVER BE
SURE.



Blocking Ciphers



Block Ciphers - AES

Advanced Encryption Standard (AES)

- A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001
- A subset of the Rijndael cipher
- **Multiple key sizes: 128, 192 or 256 bits**
- **Block size: 128 bits**

Currently considered safe to use

Attacks

Brute force attacks

- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
- On average half of all possible keys must be tried to achieve success

Time Required to Brute-force

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \cdot 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \cdot 10^{38}$	2^{127} ns = $5.3 \cdot 10^{21}$ years	$5.3 \cdot 10^{17}$ years
168	Triple DES	$2^{168} \approx 3.7 \cdot 10^{50}$	2^{167} ns = $5.8 \cdot 10^{33}$ years	$5.8 \cdot 10^{29}$ years
192	AES	$2^{192} \approx 6.3 \cdot 10^{57}$	2^{191} ns = $9.8 \cdot 10^{40}$ years	$9.8 \cdot 10^{36}$ years
256	AES	$2^{256} \approx 1.2 \cdot 10^{77}$	2^{255} ns = $1.8 \cdot 10^{60}$ years	$1.8 \cdot 10^{56}$ years

Attacks

Brute force attacks

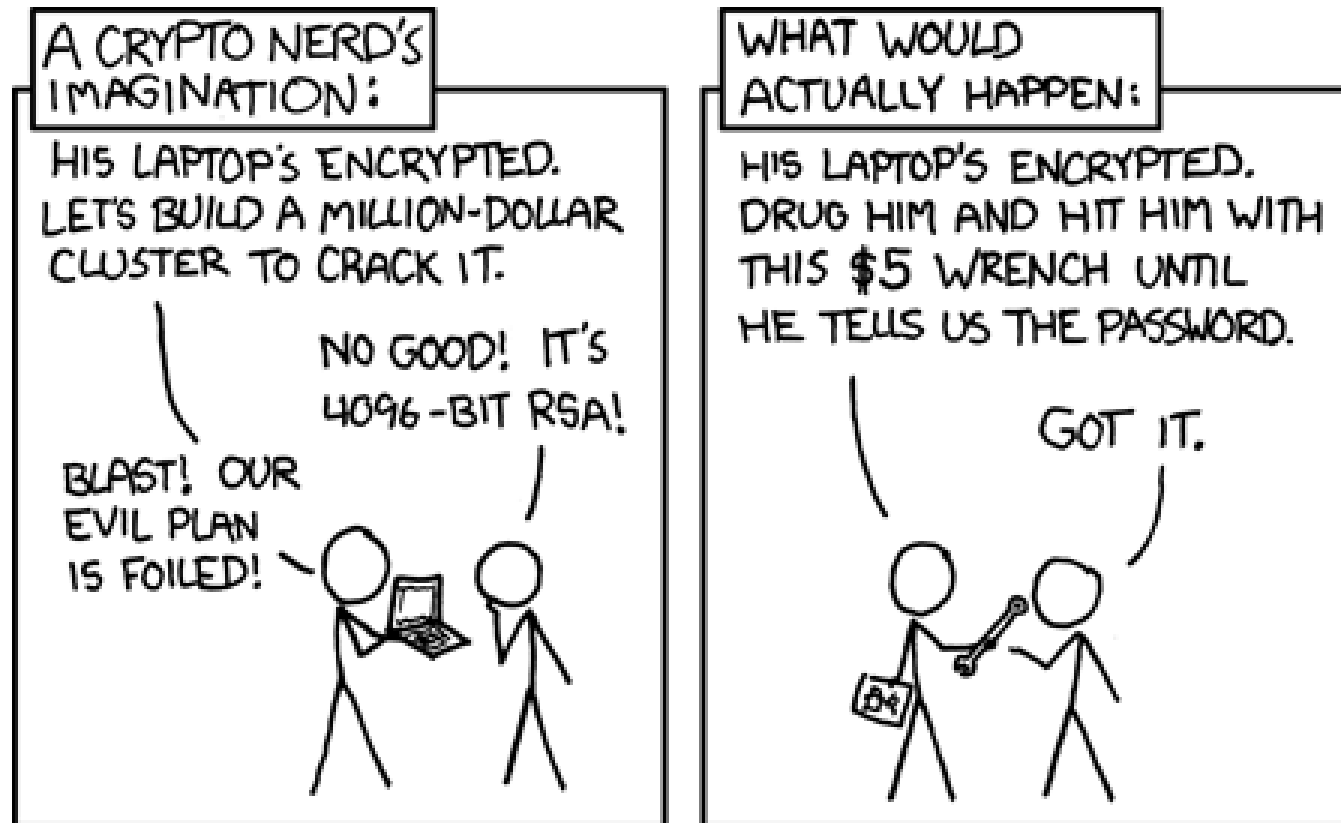
- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
- On average half of all possible keys must be tried to achieve success

Cryptanalytic attacks

- Exploit the characteristics of the algorithm and attempt to deduce a **specific plaintext** or the **key** being used
- Requires...
 - ... knowledge of the general characteristics of the plaintext
 - ... sample plaintext-ciphertext pairs

How to Break Crypto

Adi Shamir: "Crypto is typically bypassed, not penetrated"



Modes of Operation

Direct use of block ciphers is not very useful

- Attackers can build a “code book” of plaintext/ciphertext equivalents
- Message-length needs to be multiple of cipher block size

Solution! Modes of operation

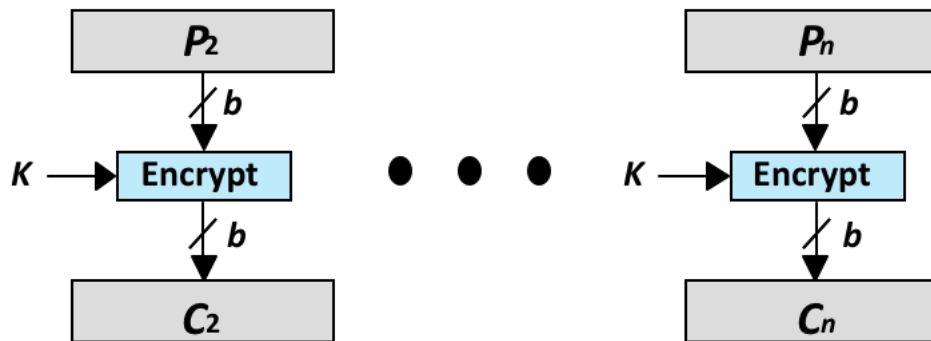
- Five standard modes

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	<ul style="list-style-type: none"> •Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	<ul style="list-style-type: none"> •General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed s bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	<ul style="list-style-type: none"> •General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	<ul style="list-style-type: none"> •Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	<ul style="list-style-type: none"> •General-purpose block-oriented transmission •Useful for high-speed requirements

ECB Mode

In electronic codebook (ECB) mode each block of plaintext is encrypted using the same key

- Easy to parallelize



Problems

- Cryptanalysts may be able to exploit regularities in the plaintext (e.g., if $p_i == p_j$ then $c_i == c_j$)
- Data patterns may remain visible

ECB Mode

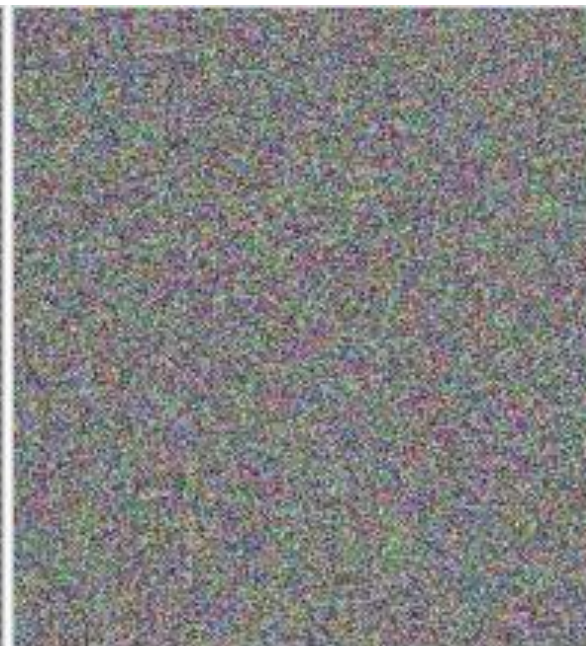
ECB mode is not recommended



Original image



Encrypted using ECB mode

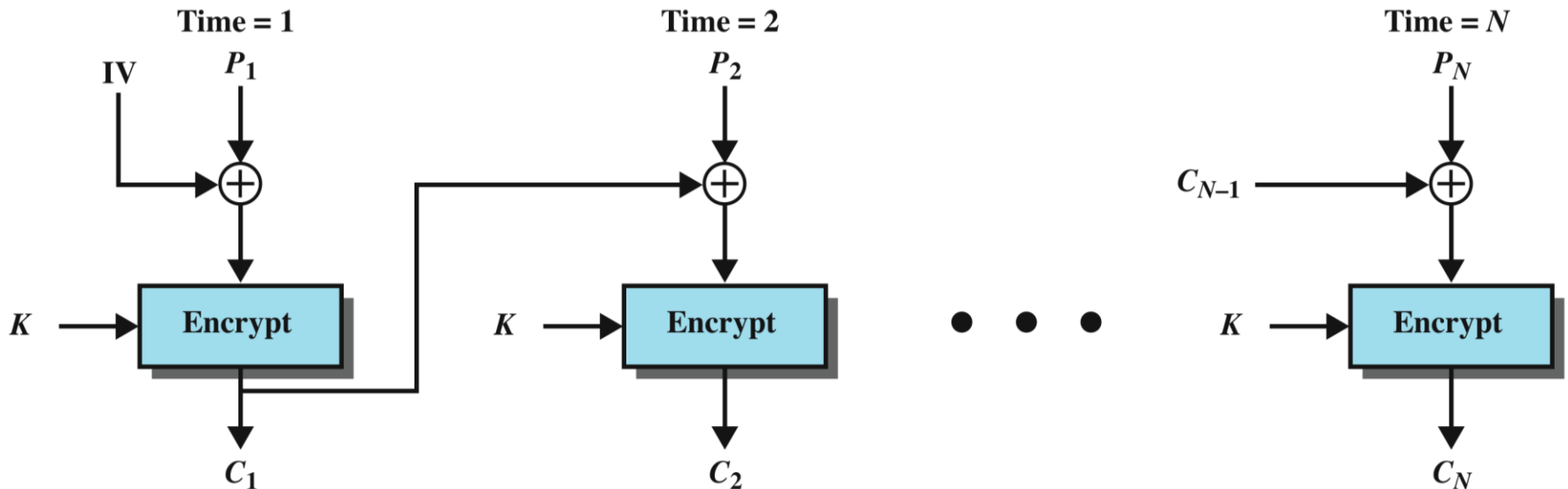


Modes other than ECB result in pseudo-randomness

CBC Mode

In Cipher Block Chaining mode the input is the XOR of the current plaintext block and the preceding ciphertext block

- **Initialization vector (IV)**
 - Must be random and must not be reused
- Not parallelizable

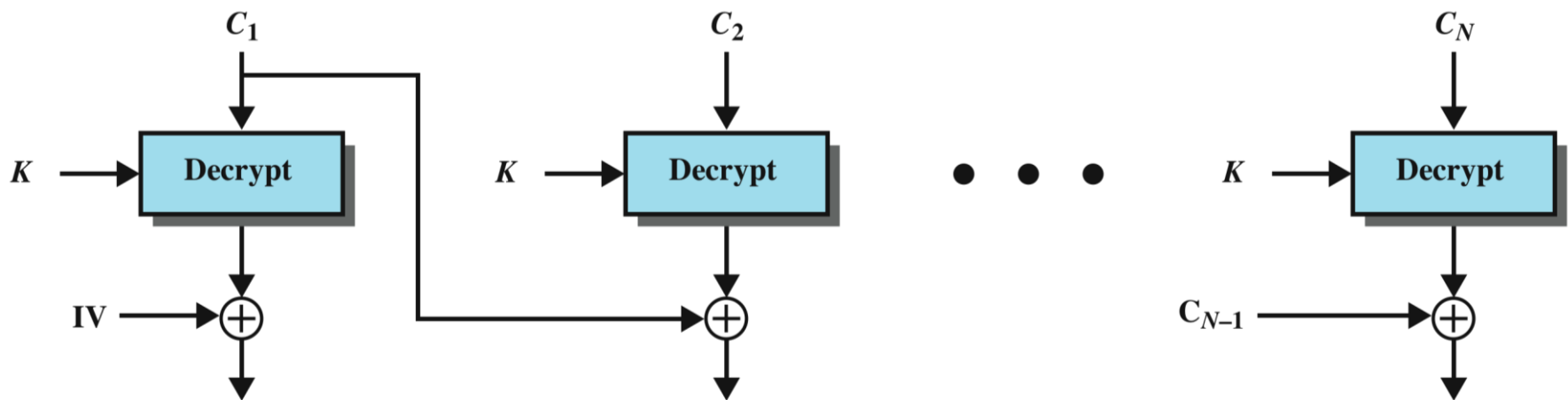


CBC Mode

During decryption the same IV must be used

- Can be transmitted with the message

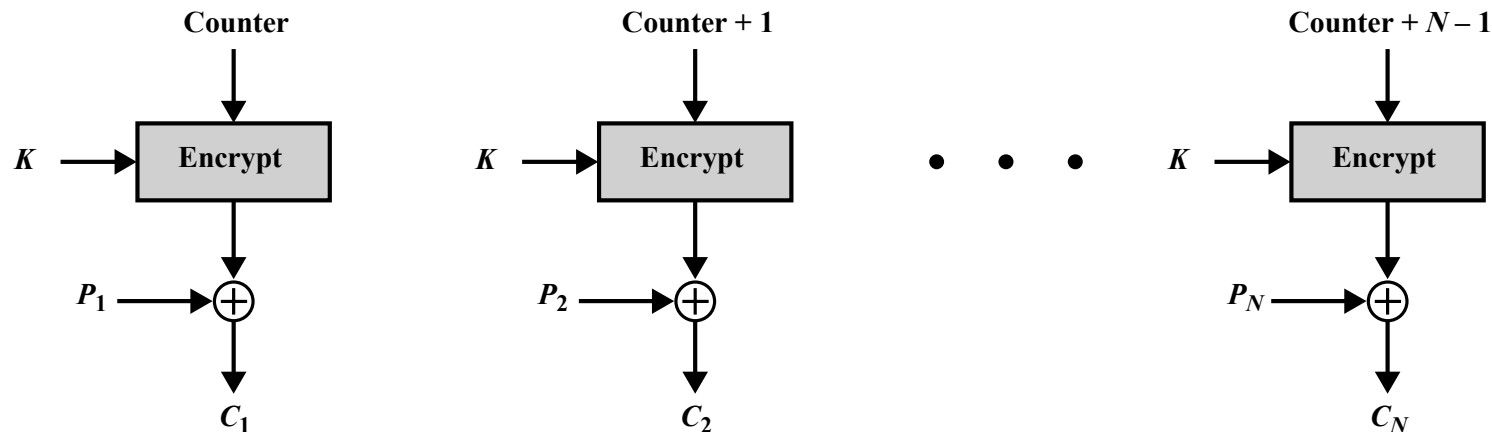
An error in a transmitted block also affects the following block but not subsequent ones



CTR Mode

Counter mode can be used to turn any blocking cipher to a stream cipher

- The counter is a combination of an integer (0..N-1) with an nonce (IV)
- **Parallelizable!**



Public-Key Encryption

Publicly proposed by Diffie and Hellman in 1976

Based on mathematical functions

- ...on the practical difficulty of factoring the product of two large prime numbers

Asymmetric

- Uses two separate keys a public and a private key
- Public key is made public for others to use

Multiple algorithms with different uses

- Establish a shared secret key
- Encrypt a message
- Digital signatures

Requirements for Public-Key Cryptosystems

Computationally easy ...

- ... to create key pairs
- ... for sender knowing public key to encrypt messages
- ... for receiver knowing private key to decrypt ciphertext

Computationally infeasible ...

- ... for opponent to determine private key from public key
- ... for opponent to otherwise recover original message

Useful if either key can be used for each role

Symmetric vs Asymmetric

Which one is best?

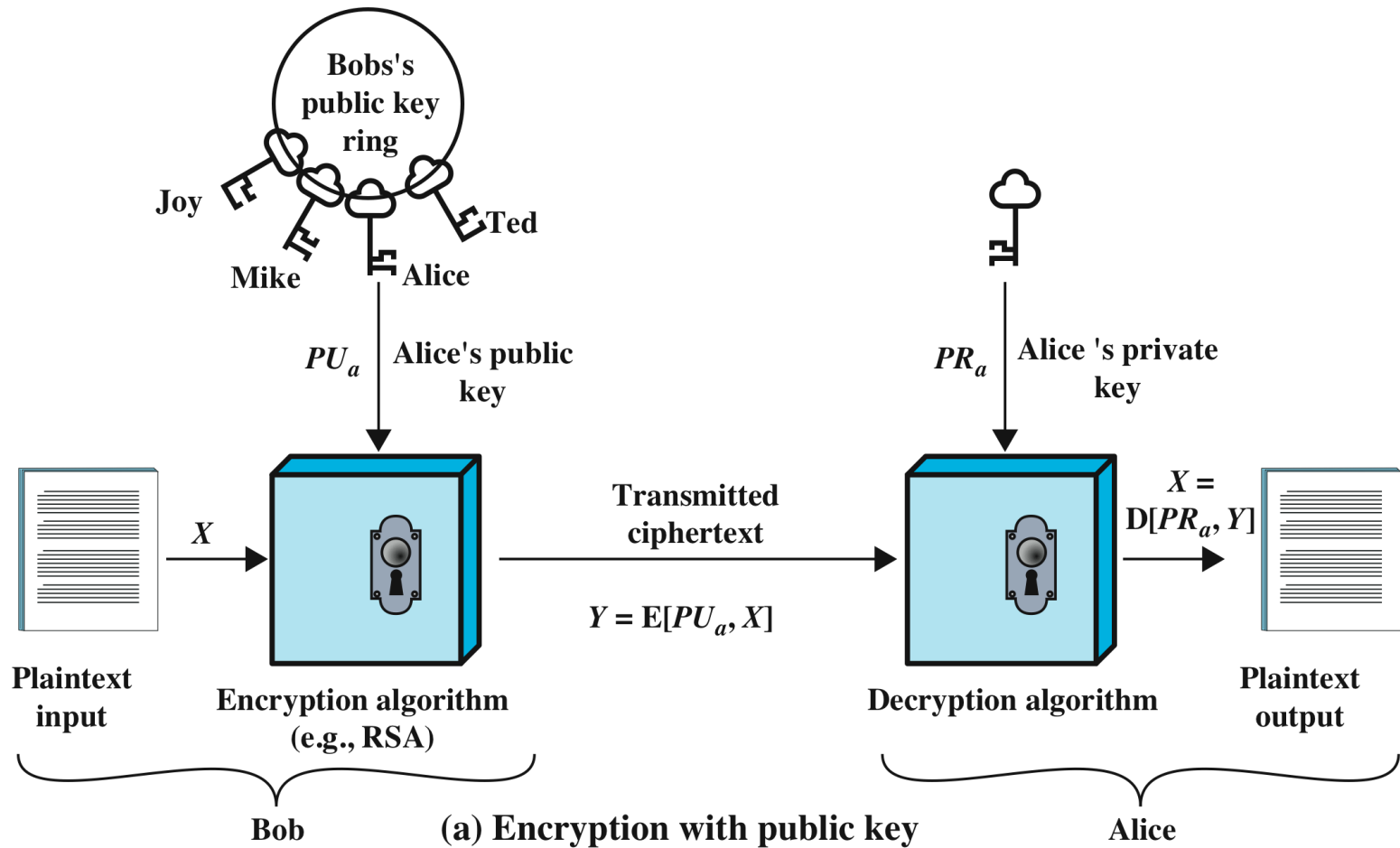
The strength of public-key cryptography depends more heavily on the length of the key

Intrinsically both offer similar guarantees against cryptanalysis

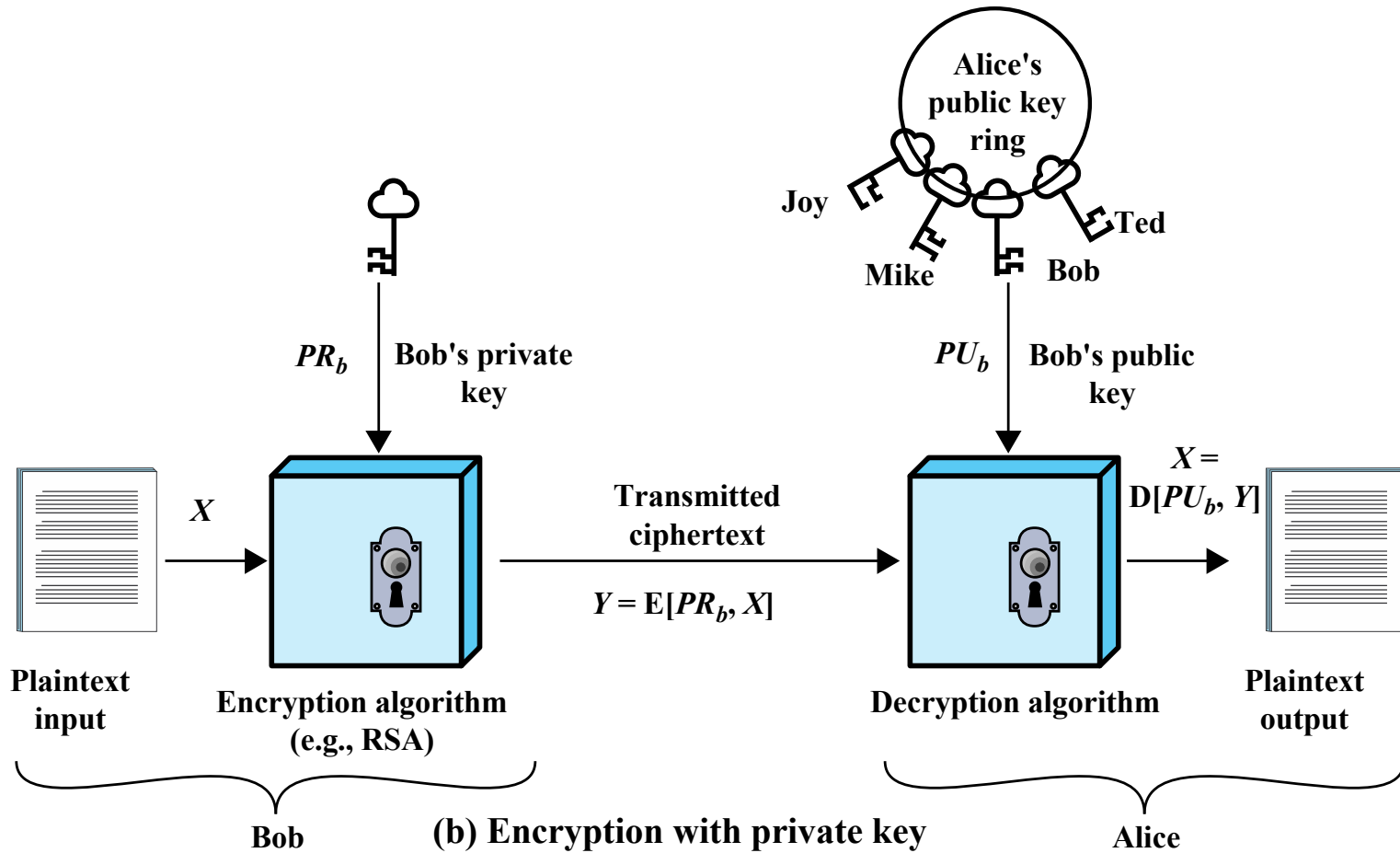
Public-key encryption is usually slower

A shared key must be kept secret, similarly to the private key, but unlike the public key

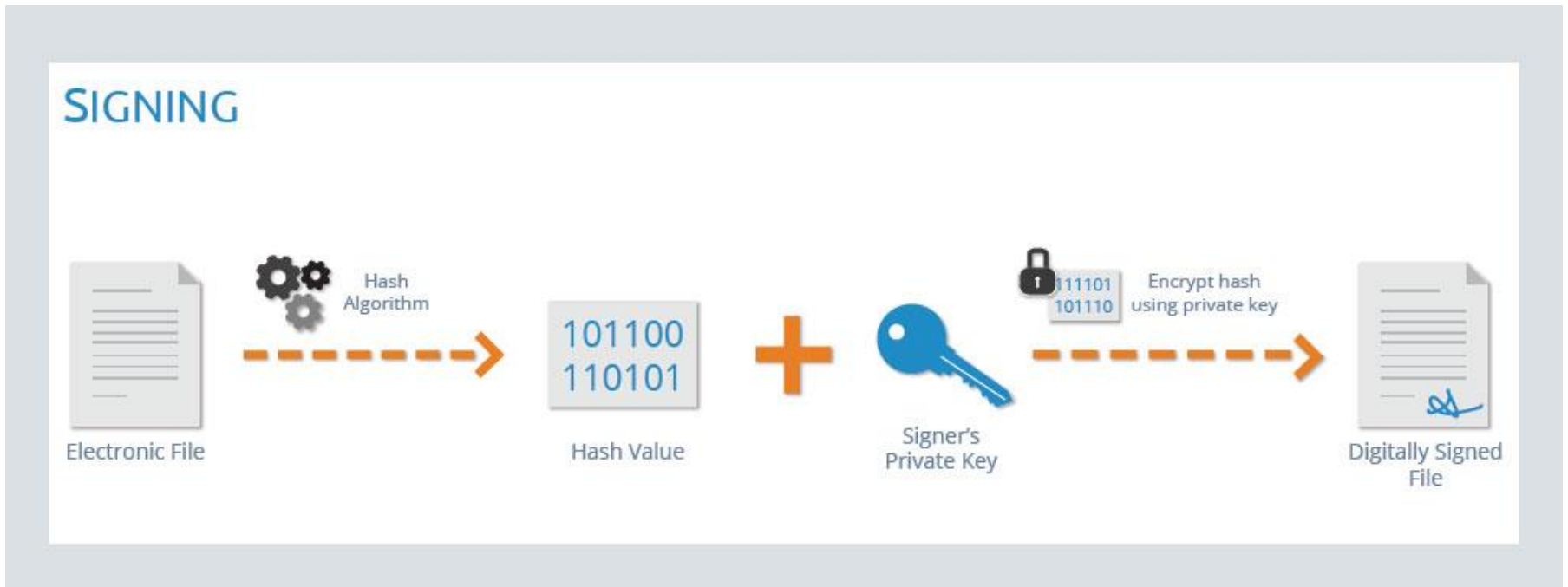
Encryption with Public Key



Encryption with Private Key



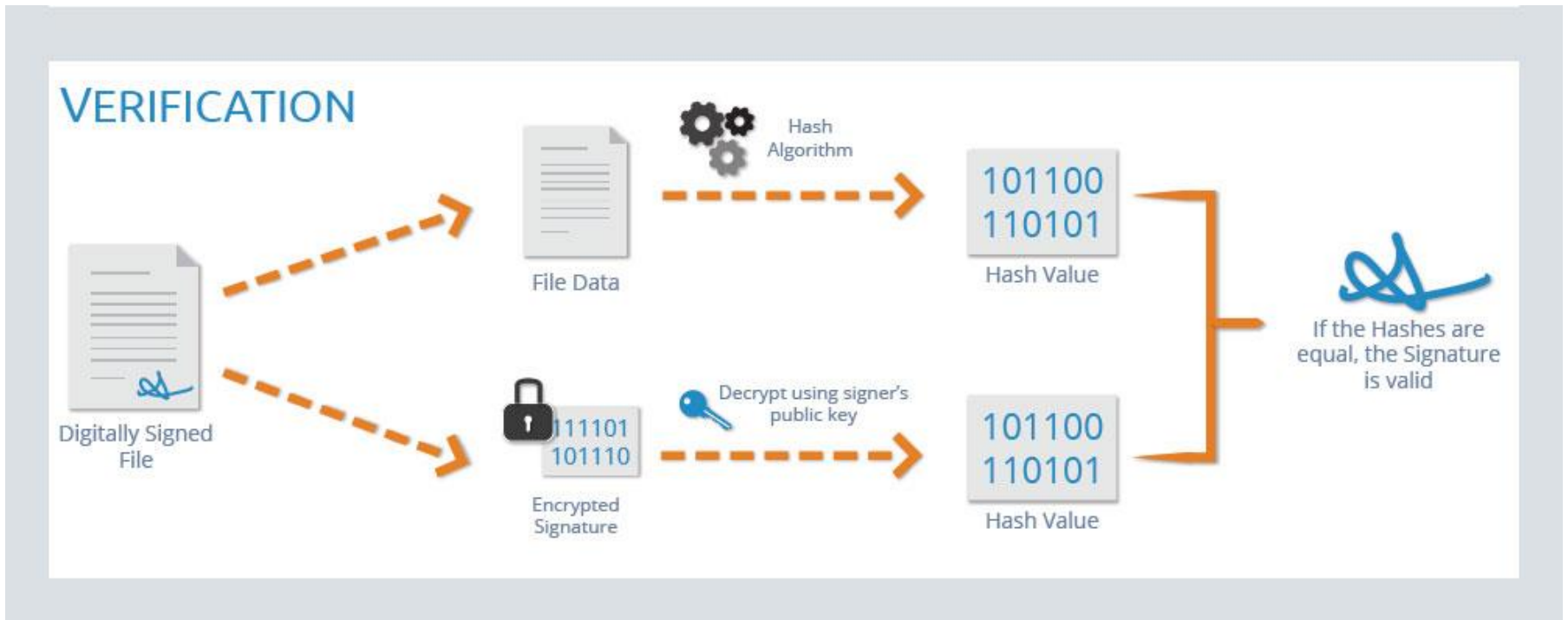
Digital Signing



Digital Signing

Verify ...

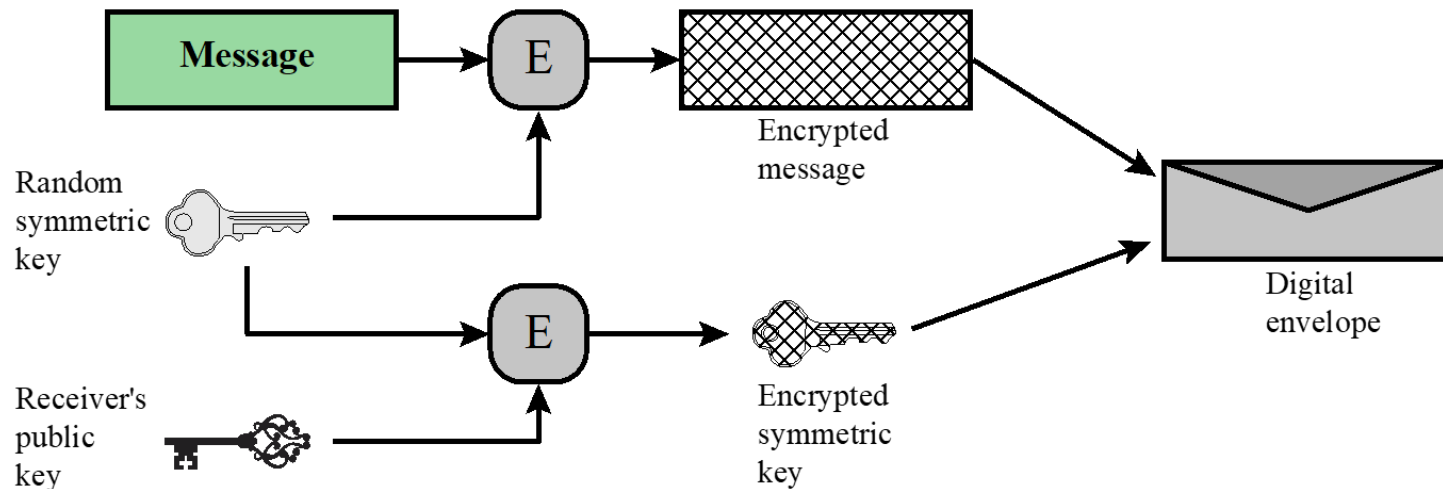
- ... the author of data
- ... the integrity of data



Digital Envelopes

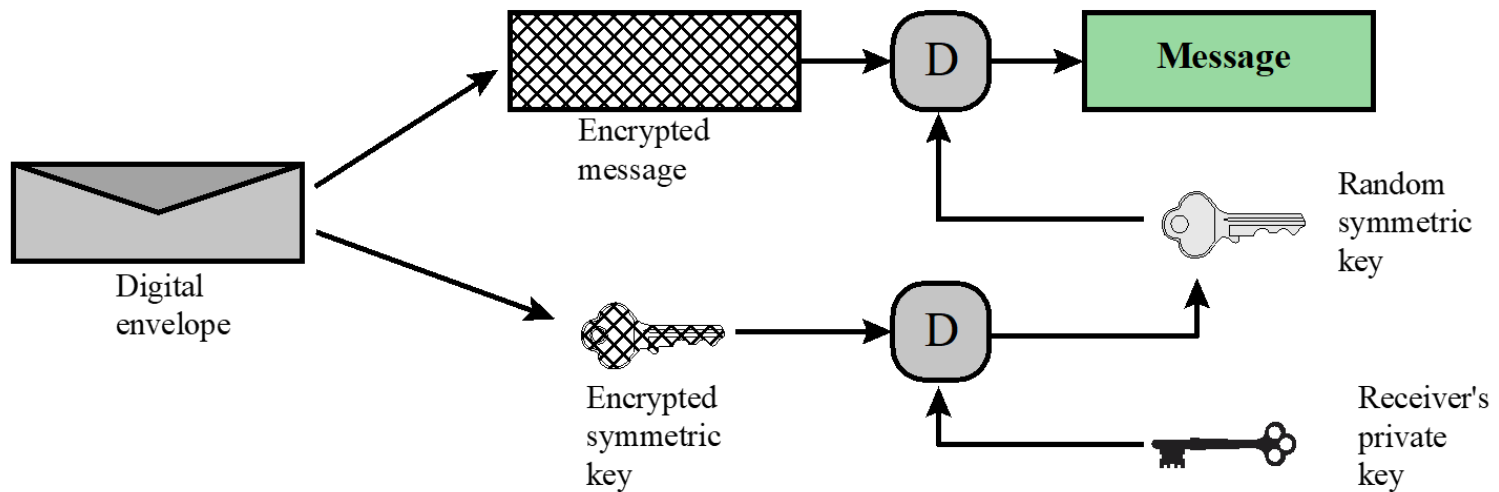
Use PK cryptography for encrypting a randomly generated symmetric key, which is used to encrypt a (large) message

- PK is only used to encrypt the key



Digital Envelopes

Opening an envelope



PK Encryption Algorithms

Diffie-Hellman key exchange algorithm

- Enables two users to securely reach agreement about a shared secret that can be used as a secret key for subsequent symmetric encryption of messages
- Limited to the exchange of the keys

RSA (Rivest, Shamir, Adleman)

- Developed in 1977
- Most widely accepted and implemented approach to public-key encryption

Elliptic curve cryptography (ECC)

- Security like RSA, but with much smaller keys

Comparison

Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
RSA	Yes	Yes	Yes
Diffie-Hellman	No	Yes	No
DSS	Yes	No	No
Elliptic Curve	Yes	Yes	Yes