Cryptographic Tools

News

- https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- https://www.welivesecurity.com/2022/09/06/worok-big-picture/

NSA Code Breaker Challenge 2024

Overview

- The Codebreaker Challenge consists of a series of tasks that are worth a varying number of points based upon their difficulty. Schools will be ranked according to the total number of points accumulated by their students.
- Solutions may be submitted at any time for the duration of the Challenge.
- This year the tasks are strictly sequential, and one must be solved before the next one becomes available.
- Each task in this year's challenge will require a range of skills. We need you to call upon all of your technical expertise, your intuition, and your common sense.

Background

- Foreign adversaries have long strived to gain an advantage against the might of the United States Armed Forces. While matching the USA on the battlefield is a costly and risky proposition, our adversaries are always looking for ways to balance the playing field. A serious and real threat is the infiltration and sabotage of military operations before the fight even breaks out.
- Fortunately, the NSA is always recruiting bright young individuals to help protect our country! In fact, a bunch of your friends graduated last year and have been busy at work in their Developmental Programs.
- You have returned to NSA on your final Cooperative Education tour and are visiting your friend Aaliyah who is currently employed full-time in the Intelligence Analysis Development Program. Intelligence Analysts are always scouring through collected Signals Intelligence (SIGINT) for threat indicators. Aaliyah recently attended a briefing that highlighted Nation-State Advanced Persistent Threats (APT) targeting our Defense Industrial Base (DIB) contractors.

Warm Up Quiz

- What do you remember from the chapter?
- http://e-mate2.s3-website-us-east-1.amazonaws.com/cryptography/cryptography.html

Key Points to Remember

- Crypto strength vs speed and resources
  - Stronger crypto takes more power and time
- Keys must be protected
- Be aware of what part of the CIA Triad + 2 you are addressing
- Don't bake your own crypto
  - Unless you are an expert crypto developer

In Class Quiz

- Based on these slides – Don't jump ahead

Two Good Crypto Tools

- Online - https://gchq.github.io/CyberChef/
- https://www.cryptool.org/en/

Encoding vs. Encryption

Some developers attempt to use encoding as encryption:

https://www.zdnet.com/article/study-shows-programmers-will-take-the-easy-way-out-and-not-implement-proper-password-security/

Hexidecimal:

- 0 – 9, A - F
- Example:
  - 54 68 69 73 20 69 73 20 74 68 65 20 73 65 63 72 65 74 20 6d 65 73 73 61 67 65

Question 1 What is the plaintext?

Encoding vs. Encryption

Base 64:

- A – Z, a –z, 0 -9, +/=
- Example:
  - VGhpcyBpcyBhbm90aGVyIHNlY3JldCBtZXNzYWdl

Question 2 What is the plaintext?

NCL Decoding Example 1

- Question 3 Decode this stolen password:
  - 3477686963684649454c4437

NCL Decoding Example 2

Question 4 Decode the stolen password

NDlmaW5lYmx1ZTkx

Encryption Terminology

- Plaintext:
  - This is the original message or data that is fed into the algorithm as input.
- Encryption algorithm:
  - The encryption algorithm performs various substitutions and transformations on the plaintext.
- Secret key:
  - The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- Ciphertext:
  - This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
- Decryption algorithm:
  - This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Encryption Categories

- Hashing
- Symmetrical encryption
- Asymmetrical encryption

Hashing

Properties of a Useful Hash Function

- Can be applied to a block of data of any size
- Produces a fixed-length output
- H(x) is relatively easy to compute for any given x
- One-way or pre-image resistant
  - Computationally infeasible to find x such that H(x) = h
- Computationally infeasible to find y ≠ x such that H(y) = H(x)
- Collision resistant or strong collision resistance
  - Computationally infeasible to find any pair (x,y) such that H(x) = H(y)

Uses of a Hash

- Used to verify file **Integrity**
  - Examples?
  - Intrusion detection?
- Used for **Confidentiality**
  - Password files – really just part of the encryption process
- Message **Authentication**

Hashing for File Integrity

- Check hash of CrypTool download on CyberChef – Sha2
  - Hash other strings and try MD5
- Intrusion detection
  - Store H(F) for each file on a system and secure the hash values

Hashing for Confidentiality

- Password files - in Labtainer – sudo cat /etc/shadow
  - Include a Salt
  - Duplicate passwords can improve chances of cracking passwords

Hashed Message Authentication

Protects against active attacks

- Verifies received message is authentic
  - Contents have not been altered
  - From authentic source
  - Timely and in correct sequence
- Can use conventional encryption
  - Only sender and receiver share a key

Message Authentication Without Confidentiality

- Message encryption by itself does not provide a secure form of authentication
- It is possible to combine authentication and confidentiality in a single algorithm by encrypting a message plus its authentication tag
- Typically, message authentication is provided as a separate function from message encryption
- Situations in which message authentication without confidentiality may be preferable include:
  - There are a number of applications in which the same message is broadcast to a number of destinations
  - An exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages
- **Thus, there is a place for both authentication and encryption in meeting security requirements**

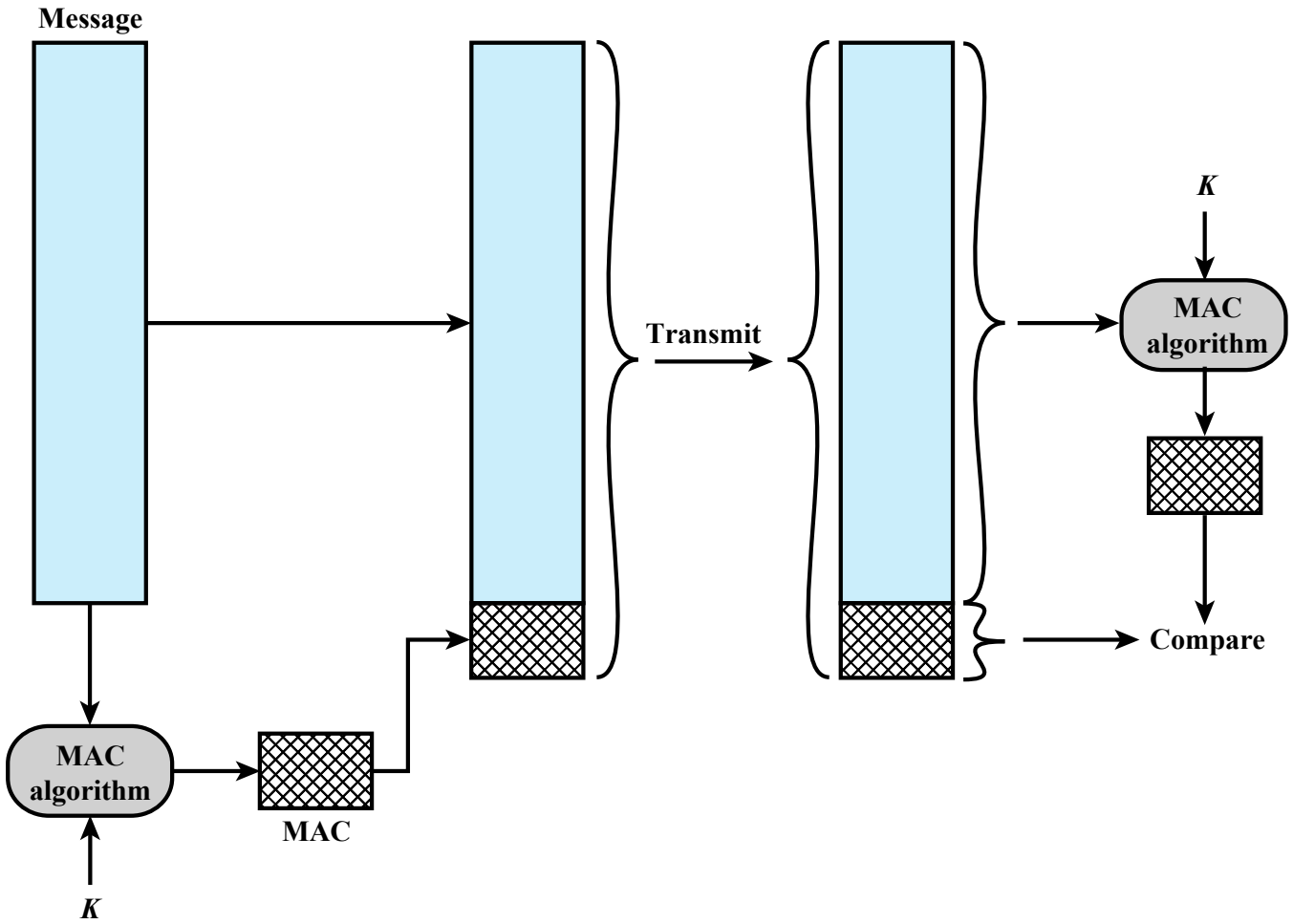


Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).

Question 5 Does this provide message integrity?

This will be discussed in more detail in PKI section.

Security of Hash Functions

- There are two approaches to attacking a secure hash function:
  - Cryptanalysis
    - Exploit logical weaknesses in the algorithm
  - Brute-force attack
    - Strength of hash function depends solely on the length of the hash code produced by the algorithm
  - Cryptool2 hash collision demos
- SHA most widely used hash algorithm

Symmetric Encryption

Classic Encryption

Symmetric Encryption

- Goal
  - Confidentiality
- Classic Encryption Algorithms
  - Substitution
    - Caesar (ROT)
    - Vingenere Cipher
    - Pigpen

Caesar Cipher (ROT3)

https://www.dcode.fr/caesar-cipher

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC

Vigenère Square

Plaintext: this is the secret message (row)
Key: wolfpack (column for encryption, row for decryption)
Ciphertext: pvtx xs vra gphgev wagdfve

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Challenge Example

Key: secretkeys (row)

Ciphertext: a eo r ltmocj

find letter, plaintext is column

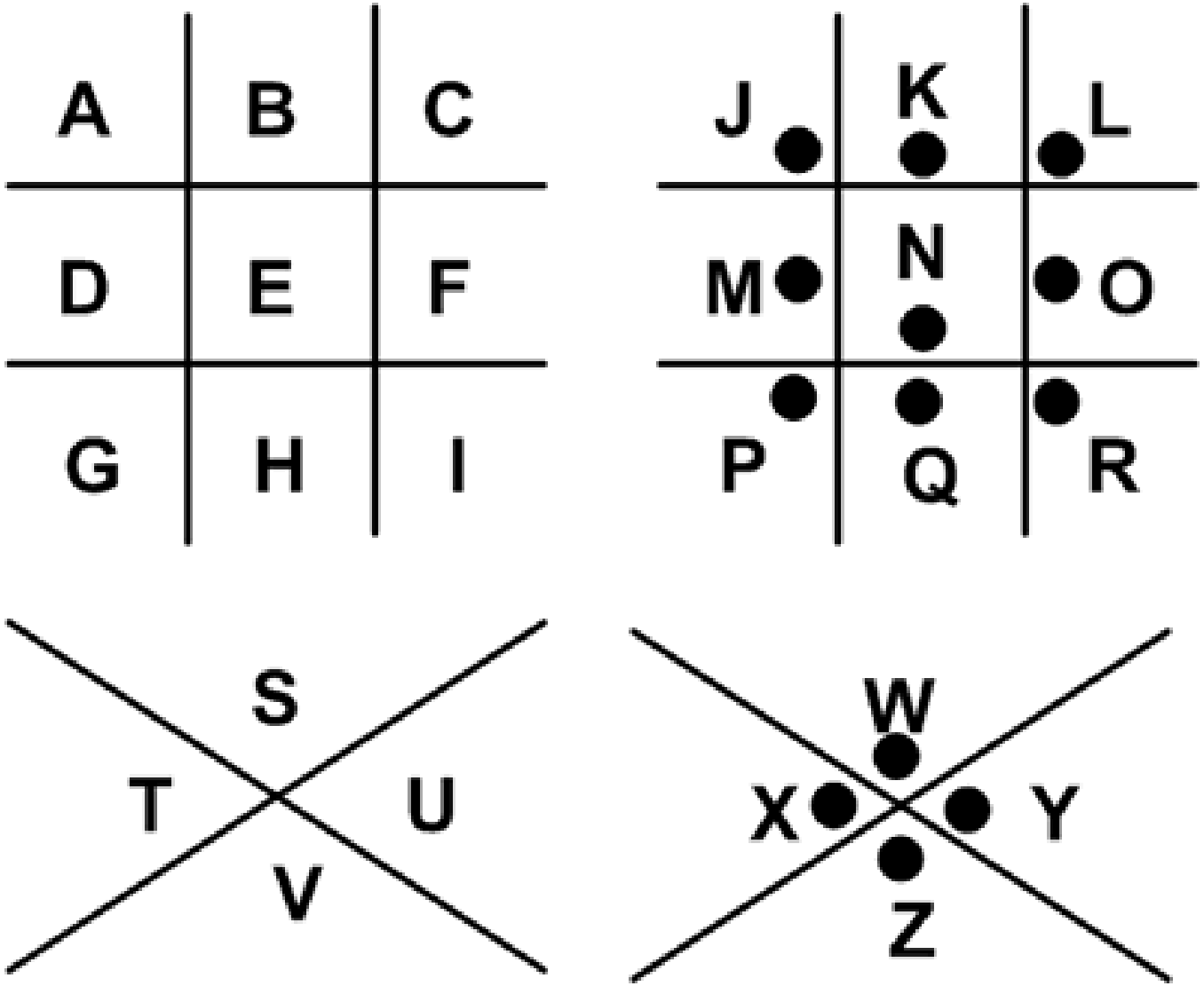
Question 6 What is the plaintext?

Link to bigger table: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher#/media/File:Vigen%C3%A8re_square_shading.svg

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Pigpen Cipher

Used by Freemasons in the 18th century



Modern Symmetric Encryption

- The universal technique for providing confidentiality for transmitted or stored data
- Also referred to as conventional encryption or single-key encryption
- Two requirements for secure use:
    - Need 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

Modern Symmetric Encryption

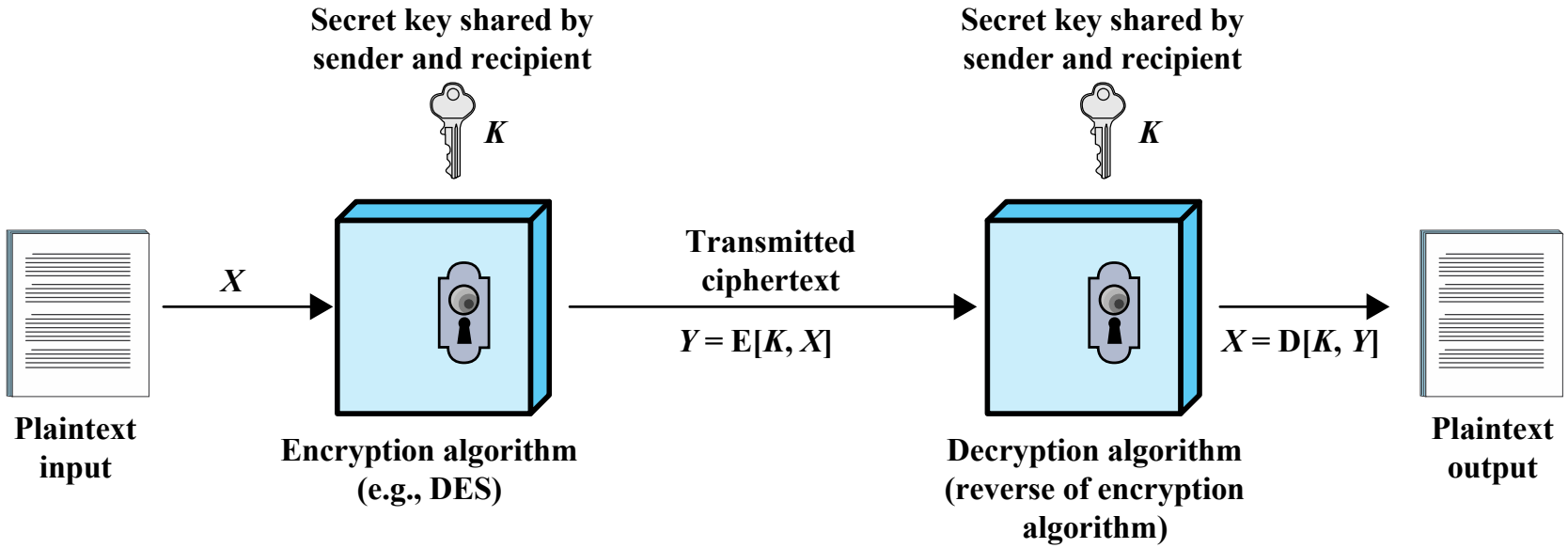


Figure 2.1 Simplified Model of Symmetric Encryption

Comparison of Three Popular Symmetric Encryption Algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

Twofish was also a finalist to replace DES and supports up to 256 bits

Average Time Required for Exhaustive Key Search

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

Attacking Symmetric Encryption

Cryptanalytic Attacks

- Rely on:
  - Nature of the algorithm
  - Some knowledge of the general characteristics of the plaintext
  - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
- If successful all future and past messages encrypted with that key are compromised

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

Practical Security Issues

- Typically symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block
- Electronic codebook (ECB) mode is the simplest approach to multiple-block encryption
  - Each block of plaintext is encrypted using the same key
  - Cryptanalysts may be able to exploit regularities in the plaintext
- Modes of operation
  - Alternative techniques developed to increase the security of symmetric block encryption for large sequences –*beyond scope of this class*
  - Overcomes the weaknesses of ECB

Block and Stream Ciphers

Block Cipher

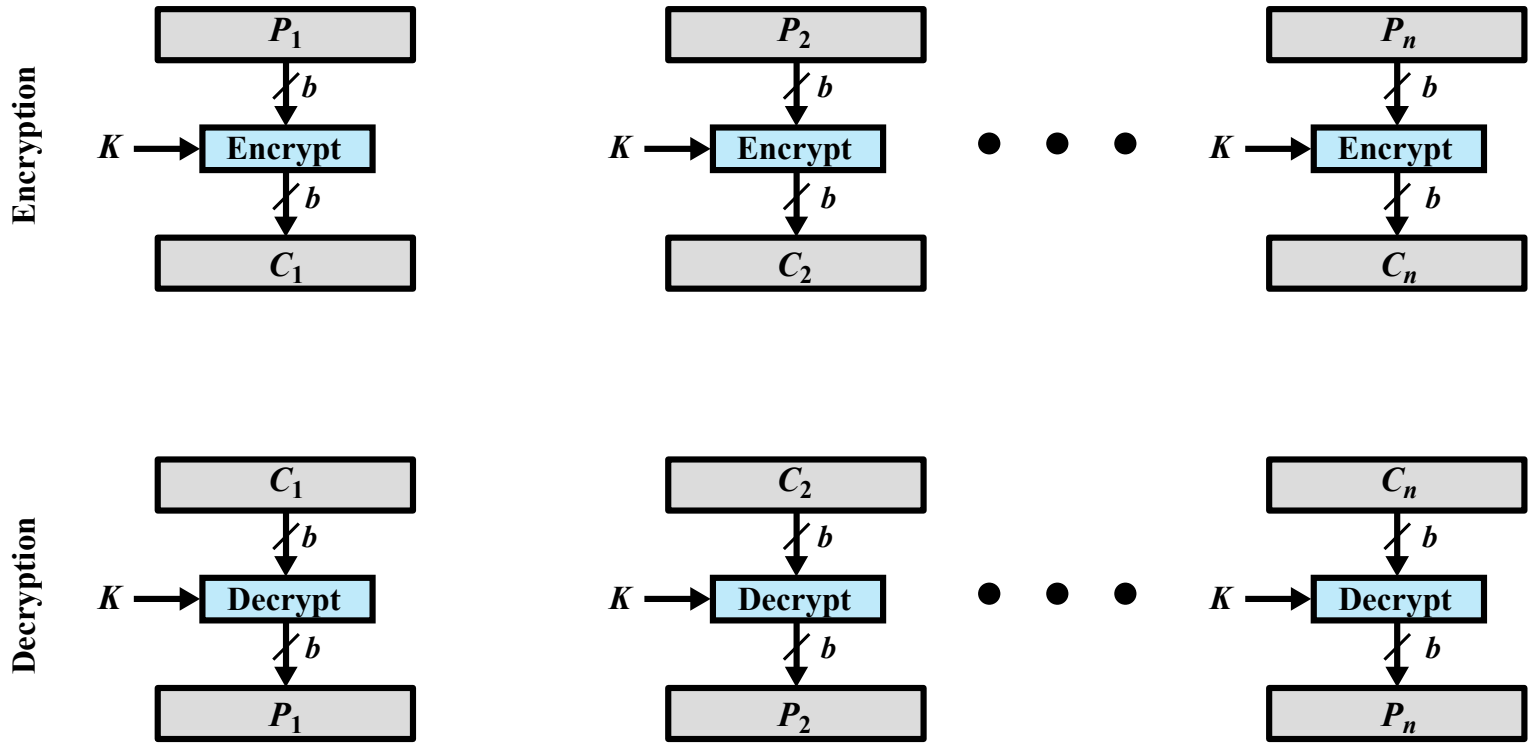
- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common

Stream Cipher

- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key

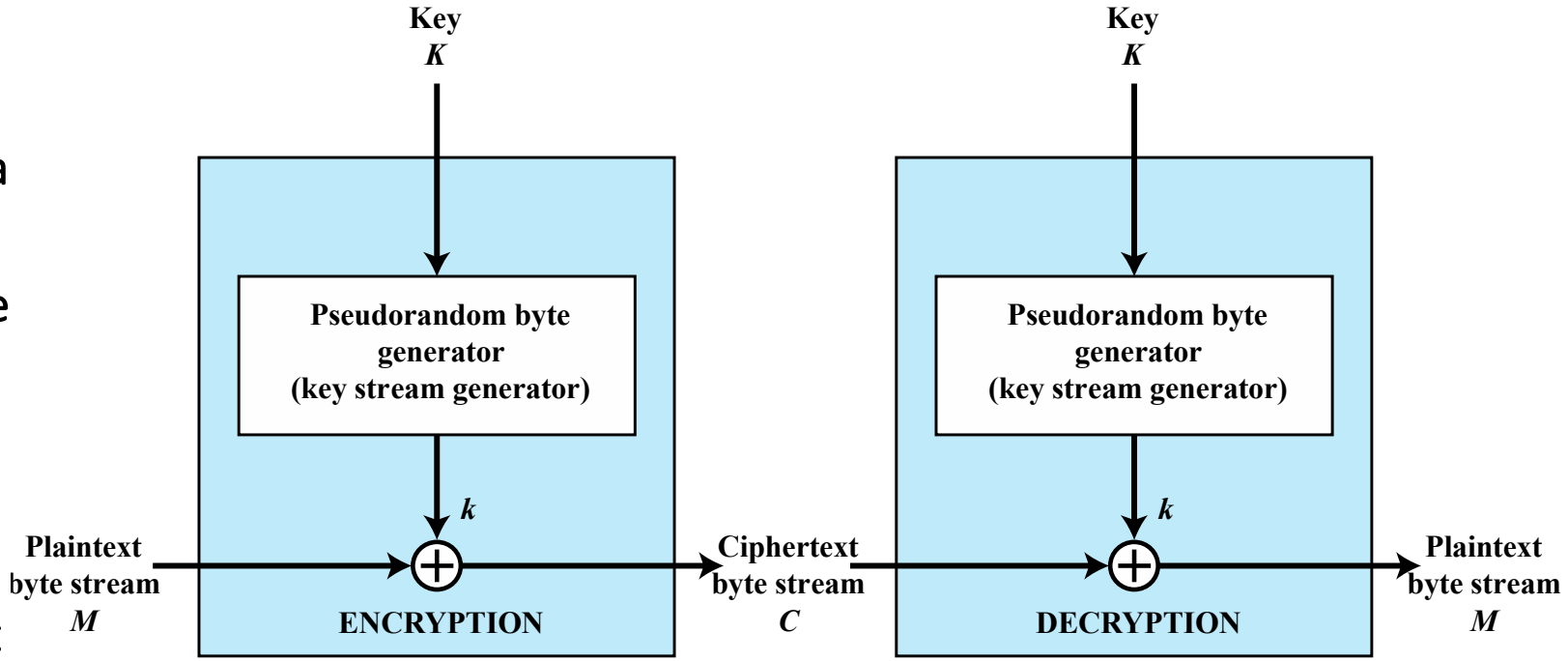
Block Cipher

- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common



Stream Cipher

- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key



Asymmetric Encryption

Asymmetric Encryption Structure

Publicly proposed by Diffie and Hellman in 1976

Based on mathematical functions

Asymmetric

- Uses two separate keys
- Public key and private key

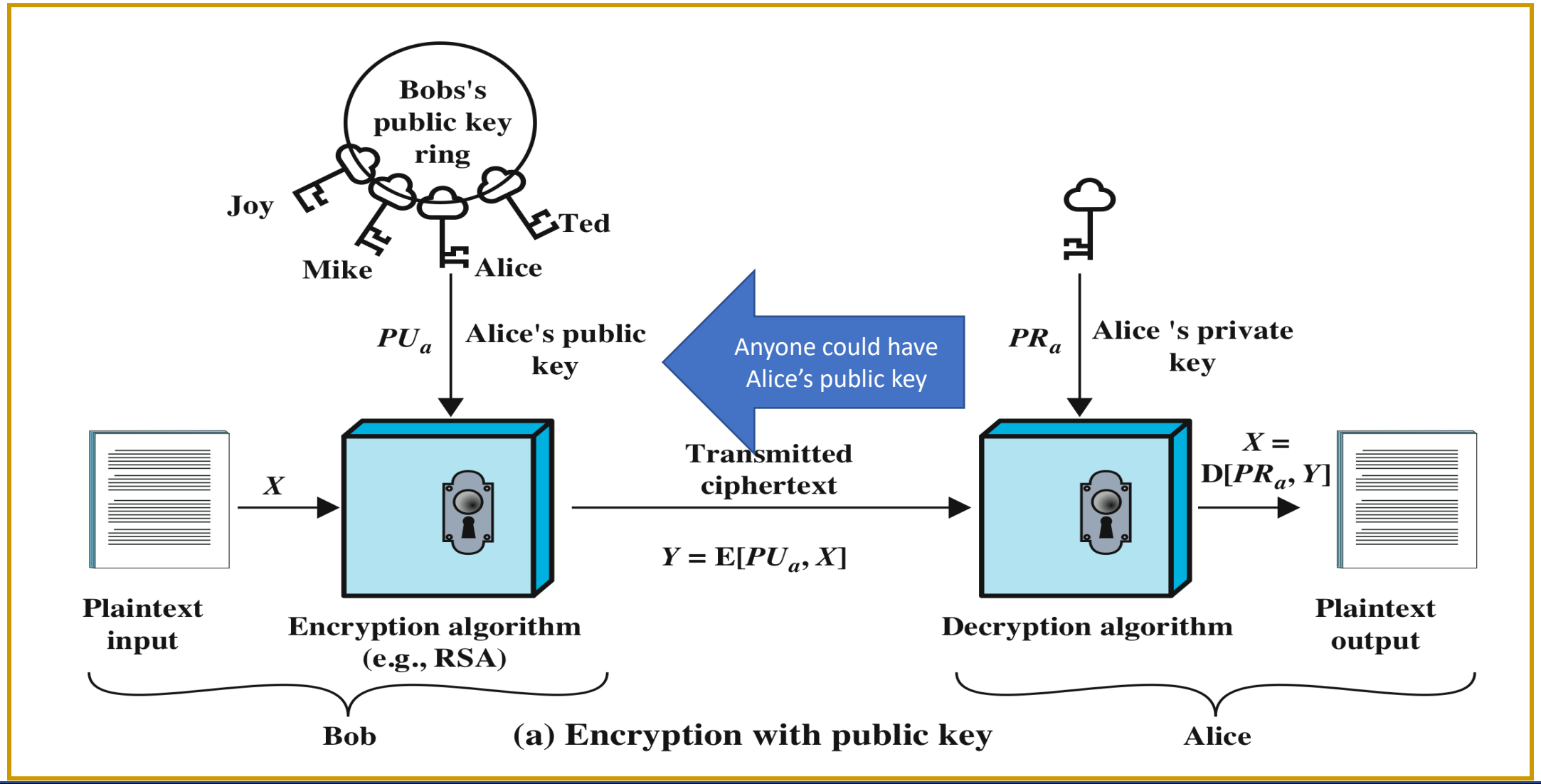
Some protocol is needed for key distribution

Using Asymmetric Encryption to Share a Symmetric Encryption Key

- Diffie-Hellman key exchange - https://www.youtube.com/watch?v=YEBfamv-_do

PGP Exercise

Public Key Encryption Without Authentication



Public-Key Crypto With Authentication

- User encrypts data using his or her own private key
- Anyone who knows the corresponding public key will be able to decrypt the message

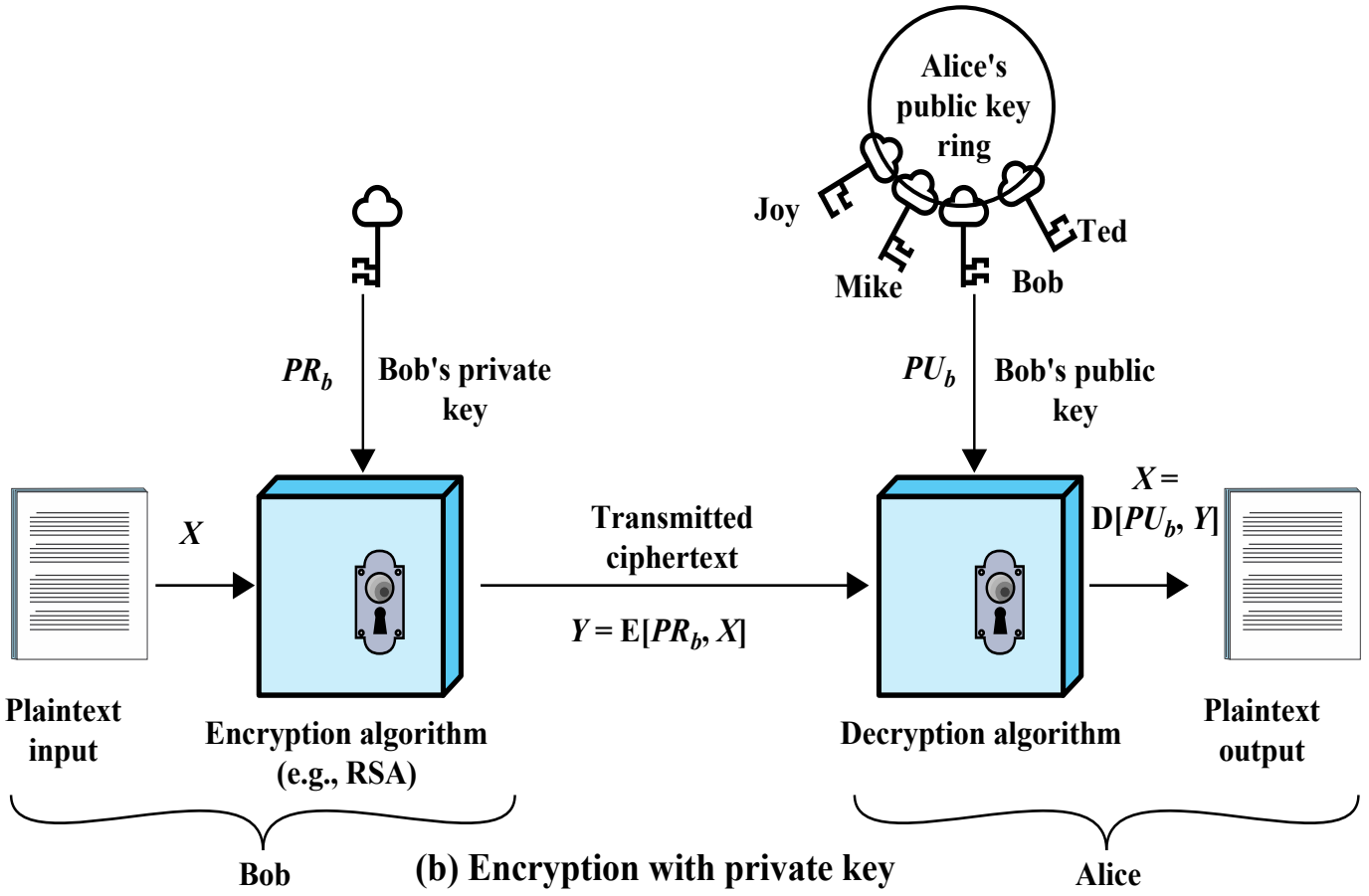


Figure 2.6 Public-Key Cryptography

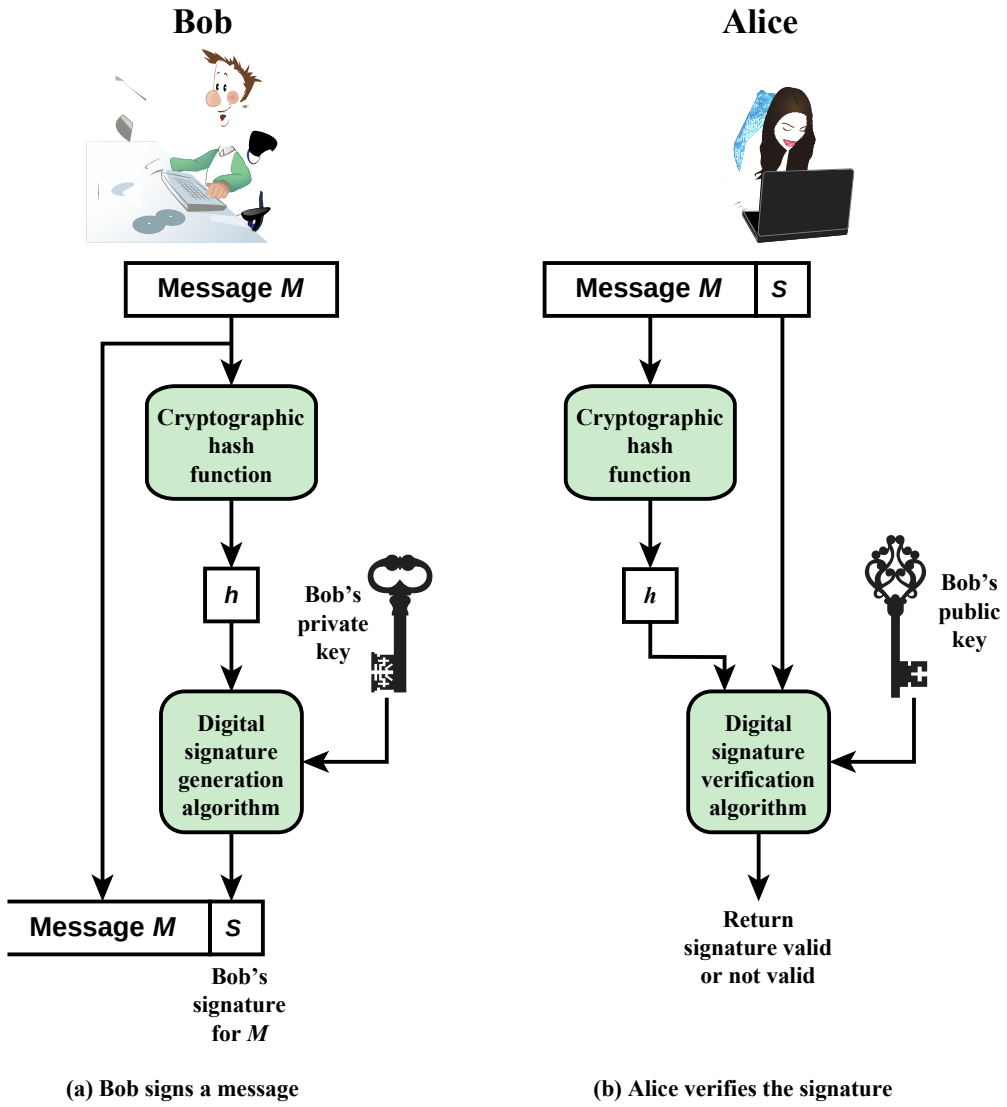
Asymmetric Encryption Algorithms

RSA (Rivest, Shamir, Adleman)	Developed in 1977
	Most widely accepted and implemented approach to public-key encryption
	Block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for some n.
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
Digital Signature Standard (DSS)	Provides only a digital signature function with SHA-1
	Cannot be used for encryption or key exchange
Elliptic curve cryptography (ECC)	Security like RSA, but with much smaller keys

Digital Signatures

- NIST FIPS PUB 186-4 defines a digital signature as:
  - ”The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation.”
- Thus, a digital signature is a data-dependent bit pattern, generated by an agent as a function of a file, message, or other form of data block
- FIPS 186-4 specifies the use of one of three digital signature algorithms:
  - Digital Signature Algorithm (DSA)
  - RSA Digital Signature Algorithm
  - Elliptic Curve Digital Signature Algorithm (ECDSA)

Digital Signature Process

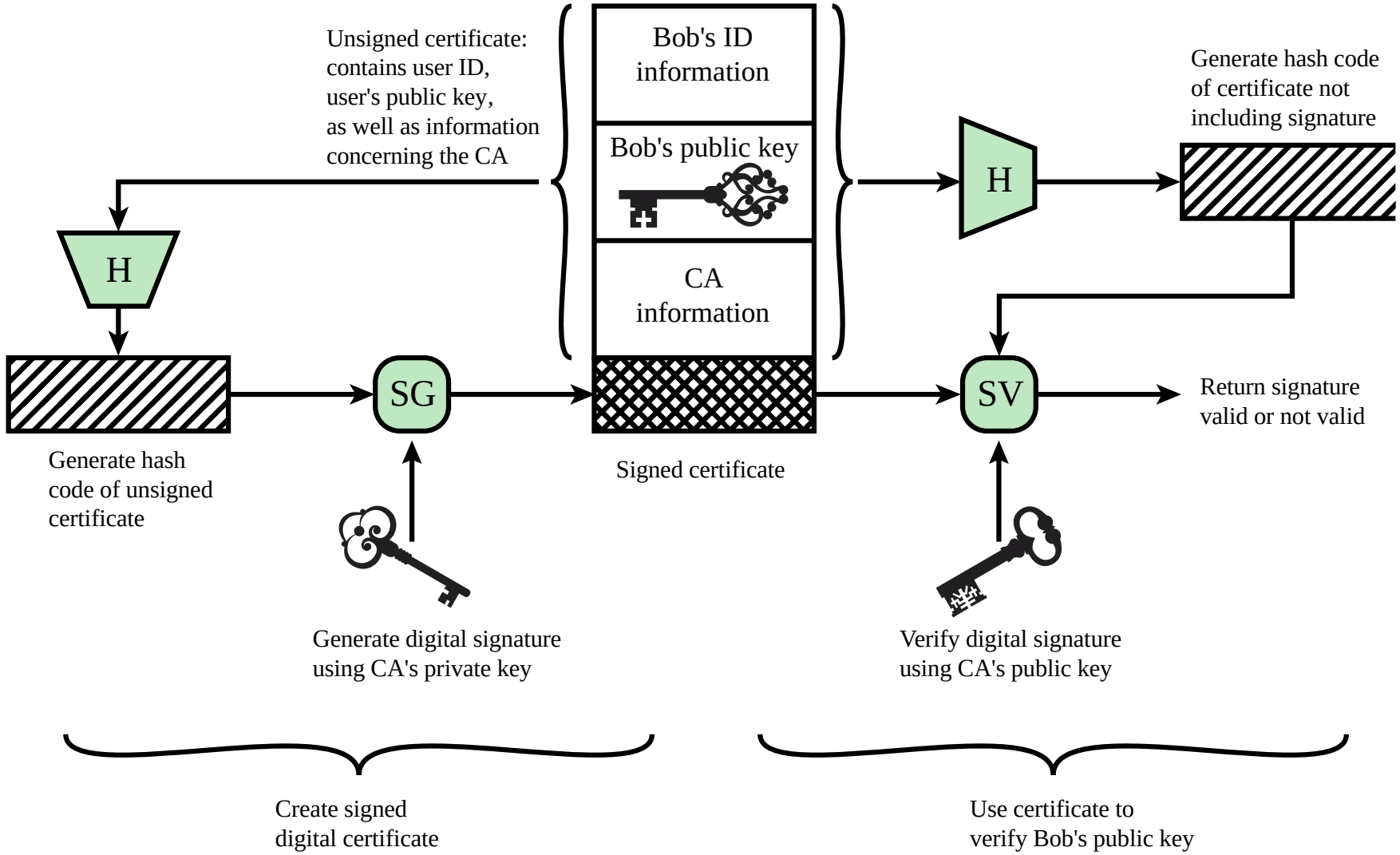


(a) Bob signs a message

(b) Alice verifies the signature

Public Key Infrastructure (PKI)

Public-Key Certificates



View Digital Certificates

- On Websites
- In Windows - certmgr

Post-Quantum PKI

https://www.cisa.gov/uscert/ncas/current-activity/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum

Random Numbers Generators

Uses include generation of:

- Keys for public-key algorithms
- Stream key for symmetric stream cipher
- Symmetric key for use as a temporary session key or in creating a digital envelope
- Handshaking to prevent replay attacks
- Session key

Random Number Requirements

Randomness

- Criteria:
  - Uniform distribution
    - Frequency of occurrence of each of the numbers should be approximately the same
  - Independence
    - No one value in the sequence can be inferred from the others

Unpredictability

- Each number is statistically independent of other numbers in the sequence
- Opponent should not be able to predict future elements of the sequence on the basis of earlier elements

Insecure Random Number Generation

- java.util.Random is not secure
  - https://intellipaat.com/community/31529/difference-between-java-util-random-and-java-security-securerandom
- Don't bake your own
  - https://owasp.org/www-community/vulnerabilities/Insecure_Randomness

Practical Encryption Applications

Common to encrypt data in transit

- VPNs
- HTTPS
- TLS

Less common to encrypt data at rest

- There is often little protection beyond domain authentication and operating system access controls
- Data are archived for indefinite periods
- Even though erased, until disk sectors are reused data are recoverable

Approaches to encrypt data at rest:

- Use a commercially available encryption package
- Back-end appliance
- Library based tape encryption
- Background laptop/PC data encryption

Steganography

Kali stego demonstration

Module 4 Assignment

- Complete the template AND spreadsheet
- Save them in their original directory on the VM