NCC education®
Awarding
Great British
Qualifications

Network Security and Cryptography

Topic 3: Cryptographic Techniques

Lecture 1

Asymmetric Cryptography

Unit Roadmap

- Introduction to Network Security and Cryptography
- **Cryptography Techniques**
- Operating System Security and Vulnerabilities
- Software Vulnerabilities and attacks
- Network Security and Defense
- Email and Web Security
- Firewalls
- VLAN and VPN
- Wireless Security
- Information Security Management

Scope and Coverage

This topic will cover:

- Asymmetric Cryptography
- Hash Function/digital signatures
- Message Authentication Code

Learning Outcomes

By the end of this topic students will be able to:

- Demonstrate a systematic understanding of the concept of cryptography.
- Understand the asymmetric key encryption principles.
- Understand in detail hash function and message authentication code.

Recap on Last Topic

- Symmetric Cryptography: single secret key between the two communicating entities.
- Modern ciphers are based on mathematic and classified as block and stream ciphers.
- Block ciphers use algorithms to encrypt and decrypt a fixed-size block of plaintext and ciphertext.
- Stream ciphers continuously encrypt any amount of data as it is presented, usually by mathematically combining the data with a keystream.
- The key length is crucial in cryptography as longer keys increase the resistance to attack.
- Sharing a key between two parties over an insecure communication channel is the fundamental issue in symmetric algorithms.

Quiz

1. Which type of traditional symmetric encryption involves replacing each plaintext character with a corresponding ciphertext character?
   a) Transposition cipher
   b) Substitution cipher **Correct Answer**
   c) RSA algorithm
   d) ECC (Elliptic Curve Cryptography)

Quiz

2. In a transposition cipher, what is the primary operation used to encrypt the plaintext?

a) Character substitution

b) XOR operation

c) Reordering of characters **Correct Answer**

d) Bitwise AND operation

Quiz

3. What is the default key length used in the Advanced Encryption Standard (AES)?

a) 64 bits

b) 128 bits **Correct Answer**

c) 256 bits

d) 512 bits

Quiz

4. Which modern symmetric encryption technique is based on a Feistel network structure?

a) DES (Data Encryption Standard)

b) AES (Advanced Encryption Standard)

c) A & B **Correct Answer**

d) RSA (Rivest-Shamir-Adleman)

Quiz

5. How does a stream cipher operate in encrypting data?

a) Processes data in fixed-size blocks

b) Utilizes a key stream to encrypt individual bits or bytes

c) Relies on a complex substitution process **Correct Answer**

d) Requires multiple rounds of transposition

Introduction

“Every Egyptian received two names, which were known respectively as the true name and the good name, or the great name and the little name; and while the good or little name was made public, the true or great name appears to have been carefully concealed.”

—The Golden Bough, Sir James George Frazer

Frazer J. G. (2020) *The Golden Bough: Volume 3.* Outlook Verlag

Symmetric Cryptography

- Traditional symmetric/private/secret/single key cryptography uses one key.
- Shared by both sender and receiver.
- If this key is disclosed communications are compromised.
- Hence does not protect the sender from the receiver forging a message & claiming is sent by sender.

How To Exchange Keys?

- One shared secret key per pair of users that want to communicate.

- How to share a secret key:
  - ✓ Trusted Third Party (TTP)
  - ✓ Key Distribution Center (KDC)
  - ✓ Diffie-Hellman (DH) protocol

Trusted Third Party (TTP)

- Trusted Third Party or Trusted Third-Party Service Provider, is an entity or organization that plays a crucial role in facilitating secure and trustworthy communication.
- Each user has a shared secret key with the TTP.
- Yahalom protocol is a cryptographic protocol that provides secure authentication and key distribution using TTP.

Yahalom Protocol Using TTP

- If Alice (A) initiates the communication to Bob (B) with S is a server trusted by both parties, the protocol can be specified as follows using security protocol notation:
  - A and B are identities of Alice and Bob respectively
  - K_{AS} is a symmetric key known only to A and S
  - K_{BS} is a symmetric key known only to B and S
  - N_A and N_B are nonces generated by A and B respectively
  - K_{AB} is a symmetric, generated key, which will be the session key of the session between A and B

Yahalom Protocol Using TTP

- Alice sends a message to Bob requesting communication.

$$A \rightarrow B : A, N_A$$

- Bob sends a message to the Server encrypted under K_{BS}.

$$B \rightarrow S: B, \{A, N_A, N_B\}_{K_{BS}}$$

- The Server sends to Alice a message containing the generated session key K_{AB} and a message to be forwarded to Bob.

$$S \rightarrow A: \{B, K_{AB}, N_A, N_B\}_{K_{AS}}, \{A, K_{AB},\}_{K_{BS}}$$

Yahalom Protocol Using TTP

- Alice forwards the message to Bob and verifies N_A has not changed. Bob will verify N_B has not changed when he receives the message.

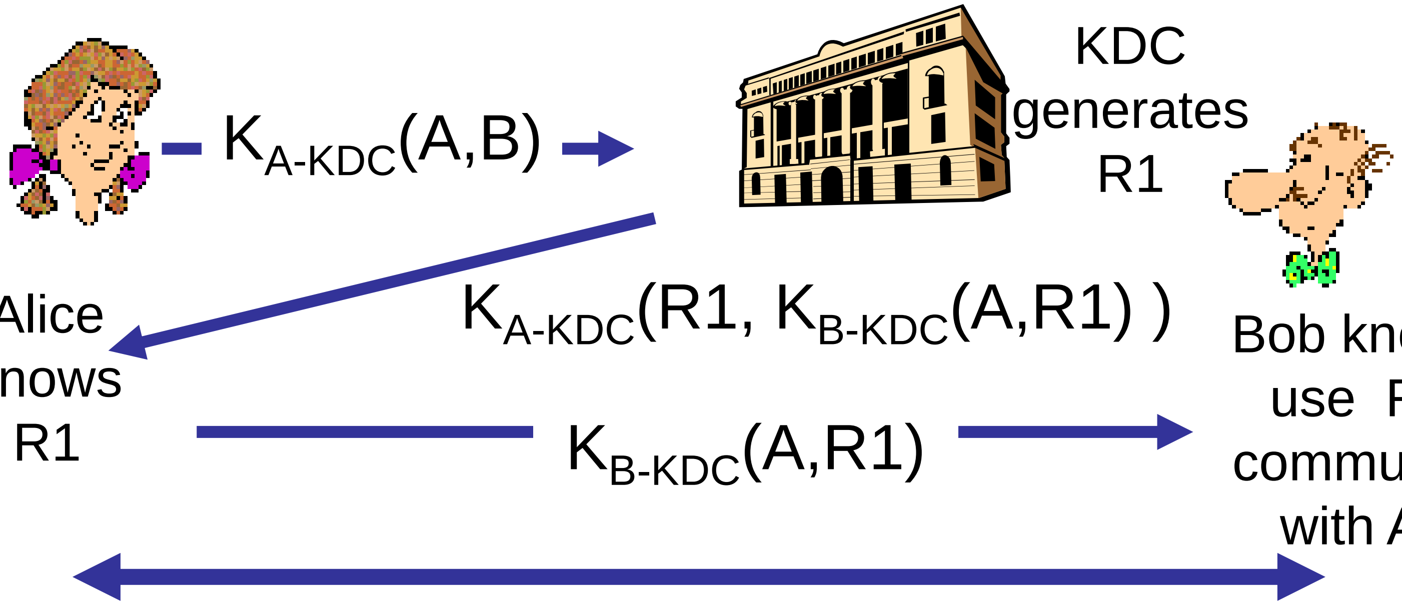
$$A \rightarrow B: \{A, K_{AB},\}_{K_{BS}}, \{N_B\}_{K_{AB}}$$

Key Distribution Center (KDC)

- Alice, Bob need shared symmetric key.
- KDC: server shares different secret key with each registered user (many users).
- Alice, Bob know their own symmetric keys, $K_{A\text{-}KDC}$ $K_{B\text{-}KDC}$, for communicating with KDC.

How does KDC allow Bob, Alice to determine shared symmetric secret key to communicate with each other?

Key Distribution Center (KDC)



$K_{A\text{-}KDC}(A,B)$

KDC generates R1

$K_{A\text{-}KDC}(R1, K_{B\text{-}KDC}(A,R1))$

Alice knows R1

$K_{B\text{-}KDC}(A,R1)$

Bob knows to use R1 to communicate with Alice

Alice and Bob communicate using R1 as *session key* for shared symmetric encryption

TTP VS KDC

Purpose:

- The primary purpose of a KDC is to facilitate authentication and secure key distribution within a specific authentication domain or network.
- KDCs are often used in authentication protocols like Kerberos, which is commonly employed in corporate and network security.
- TTP is a broader concept and can serve various roles, including identity verification, digital certificate issuance, dispute resolution, and escrow services.
- TTPs aim to provide trust and security in a wide range of online transactions and communications, beyond just authentication and key distribution.

TTP VS KDC

Scope:

- KDCs are typically specific to a particular authentication domain or network, such as an organization's internal network.
- Their function is focused on facilitating secure authentication and access control within that domain.
- TTPs can be independent entities or organizations that provide trust and security services to parties involved in various online interactions, often across different domains.
- They are more versatile and can serve in a broader range of scenarios, such as e-commerce, legal agreements, secure communications, and more.

Diffie-Hellman (DH) Key Exchange

- The Diffie-Hellman algorithm was developed by Whitfield Diffie and Martin Hellman in 1976.

- This algorithm was devised not to encrypt the data but to generate same private cryptographic key at both ends so that there is no need to transfer this key from one communication end to another.

Diffie-Hellman (DH) Key Exchange

- The main idea behind the algorithm is to agree on a key that two parties can use for a symmetric encryption, in such a way that an eavesdropper cannot obtain the key.

- It also depends on the difficulty to compute discrete logarithms.

Diffie-Hellman (DH) Key Exchange

- Advantages:
  - ✓ The sender and receiver have no prior knowledge of each other.
  - ✓ Communication can take place through an insecure channel.
  - ✓ Sharing of secret key is safe.
- Disadvantage:
  - ✓ A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

Asymmetric Cryptography

- Probably most significant advance in the 3000-year history of cryptography.
- Uses two keys – a public & a private key.
- Asymmetric since parties are not equal.
- Uses clever application of number theoretic concepts to function.
- Complements rather than replaces symmetric key crypto.
- Also known as public-key cryptography.
- Today's internet transmission is secured using on Asymmetric Encryption, particularly in TLS.

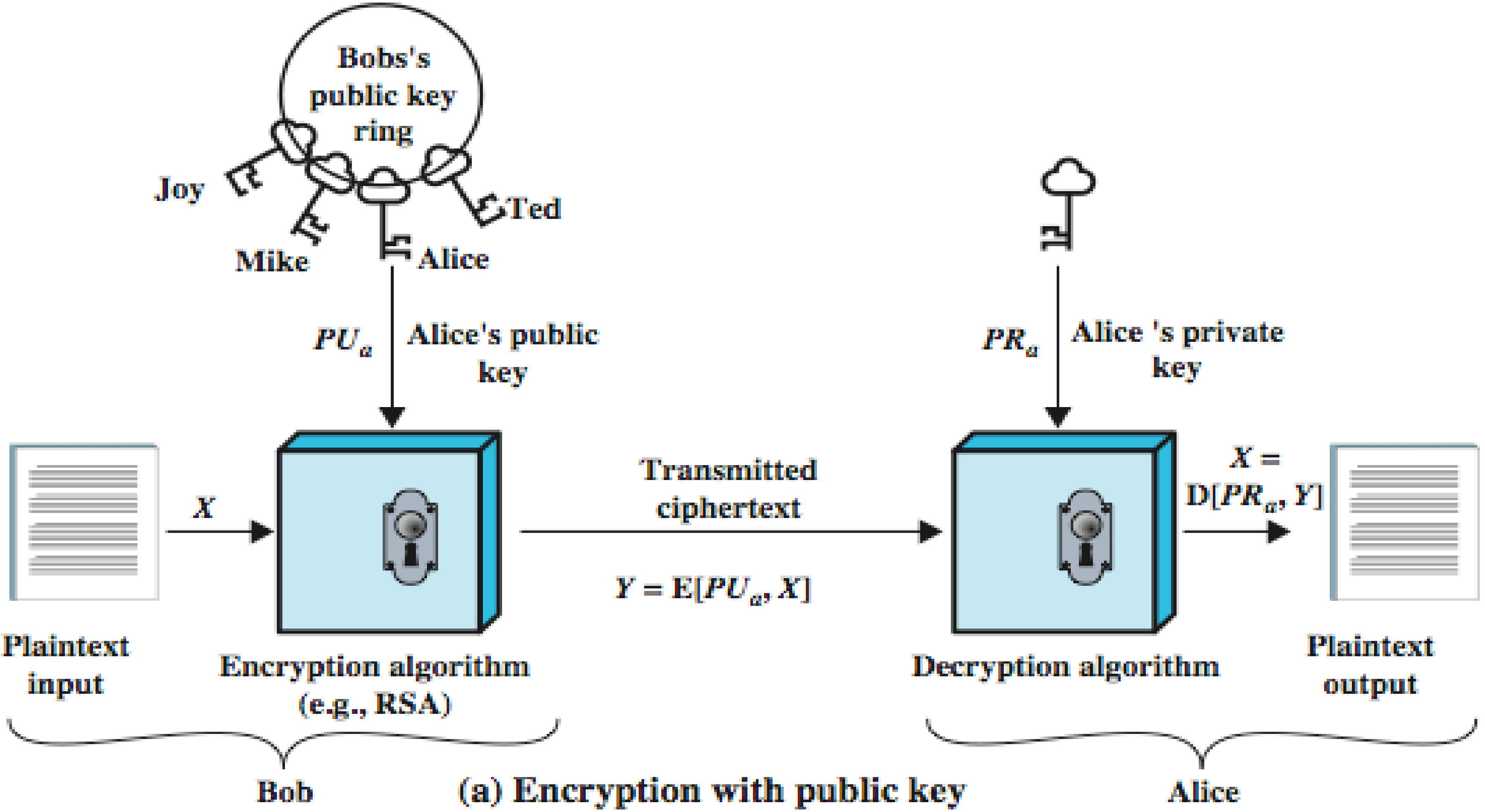
Why Asymmetric Cryptography?

- Developed to address two key issues:
  - ✓ Key distribution – how to have secure communications in general without having to trust a KDC with your key
  - ✓ Digital signatures – how to verify a message comes intact from the claimed sender
- Public invention due to Whitfield Diffie & Martin Hellman at Stanford Uni in 1976

Asymmetric Cryptography

- Public-key/two-key/asymmetric cryptography involves the use of two keys:
  - ✓ Public-key: which may be known by anybody, and can be used to encrypt messages, and verify signatures.
  - ✓ Private-key: known only to the recipient, used to decrypt messages, and sign (create) signatures.
- Infeasible to determine private key from public
- Is asymmetric because those who encrypt messages or verify signatures cannot decrypt messages or create signatures

Asymmetric Cryptography

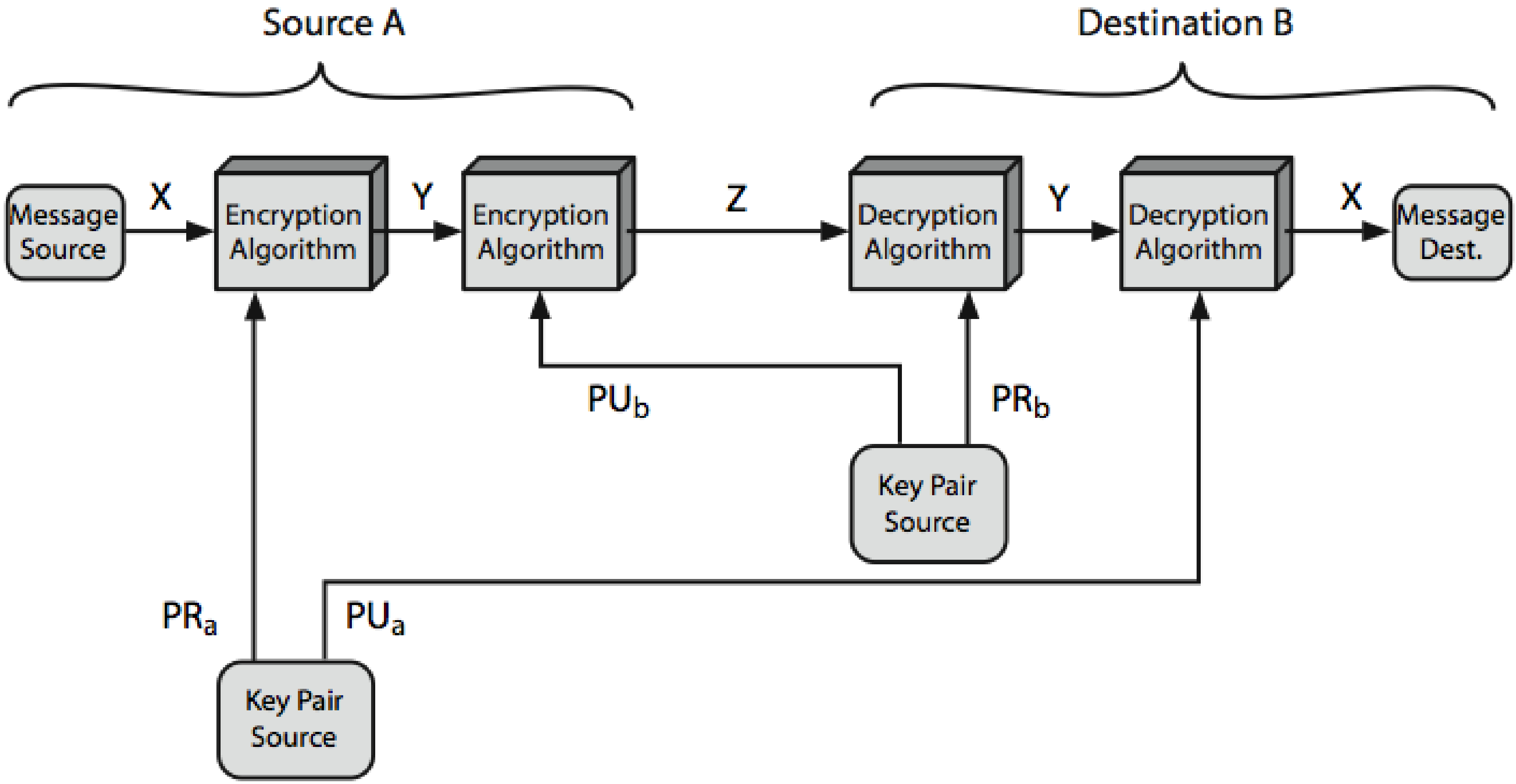


STALLINGS, W. 2022. *Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition*, Pearson.

Symmetric vs Asymmetric Crypto

Symmetric	Asymmetric
Needed to Work	
Same algorithm with same key is used for encryption and decryption	Same algorithm with different key is used for encryption and decryption
The sender and receiver must share the algorithm and key	The sender and receiver must each have one of the Matched paired key.
Needed for Security	
The key must be kept secret	One of the key must kept secret.
It must be impossible to decipher text if no other information is known	It must be impossible to decipher text if no other information is known
Knowledge of algorithm plus samples of ciphertext must be insufficient to determine the key.	Knowledge of algorithm plus one of the key plus samples of ciphertext must be insufficient to determine the other key.

Asymmetric Cryptography



STALLINGS, W. 2022. *Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition*, Pearson.

Asymmetric Crypto Applications

- Can classify uses into 3 categories:
  - ✓ Encryption/decryption (provide secrecy)
  - ✓ Digital signatures (provide authentication)
  - ✓ Key exchange (of session keys)

Asymmetric Crypto Requirements

- Public-Key algorithms rely on two keys where:
  - ✓ It is computationally infeasible to find decryption key knowing only algorithm & encryption key
  - ✓ It is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known
  - ✓ Either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms)
- These are formidable requirements which only a few algorithms have satisfied

Asymmetric Crypto Requirements

- Need a trapdoor one-way function
- One-way function has

  Y = f(X) easy

  X = f–1(Y) infeasible

- A trap-door one-way function has

  Y = fk(X) easy, if k and X are known

  X = fk–1(Y) easy, if k and Y are known

  X = fk–1(Y) infeasible, if Y known but k not known

- A practical public-key scheme depends on a suitable trap-door one-way function

Security of Asymmetric Crypto Schemes

- Like private key schemes brute force exhaustive search attack is always theoretically possible
- But keys used are too large (>512bits)
- Security relies on a large enough difference in difficulty between easy (en/decrypt) and hard (cryptanalyze) problems
- More generally the hard problem is known, but is made hard enough to be impractical to break
- Requires the use of very large numbers
- Hence is slow compared to private key schemes

RSA

- By Rivest, Shamir & Adleman of MIT in 1977
- Best known & widely used public-key scheme
- The RSA algorithm holds the following features −
  - ✓ RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
  - ✓ The integers used by this method are sufficiently large making it difficult to solve.
  - ✓ There are two sets of keys in this algorithm: private key and public key.

RSA Algorithm

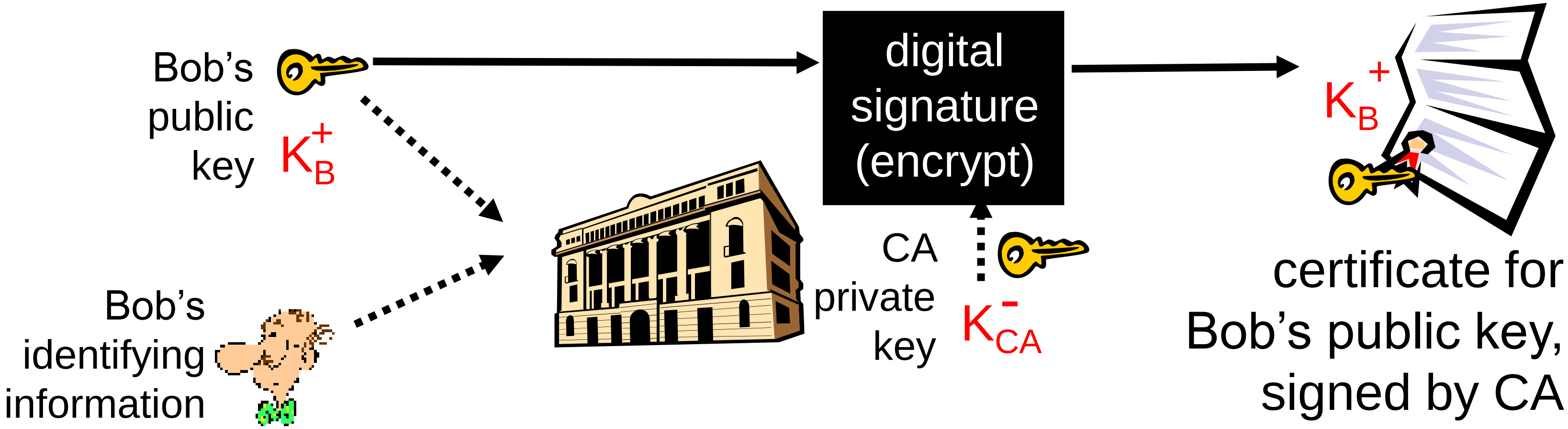
Steps of RSA algorithm:

- Step 1: Choose very large prime numbers, p and q.
- Step 2: Let N = p*q
- Step 3: Let T = (p-1)(q-1)   Euler Totient
- Step 4: Chose two number E and D where (E * D) mod T = 1.
- Step 5: Publish e and N. This is your public key.
- Step 6: Keep d and N. This is your Private Key

Certification Authorities or Public Key Infrastructure (PKI)

How to share public keys!

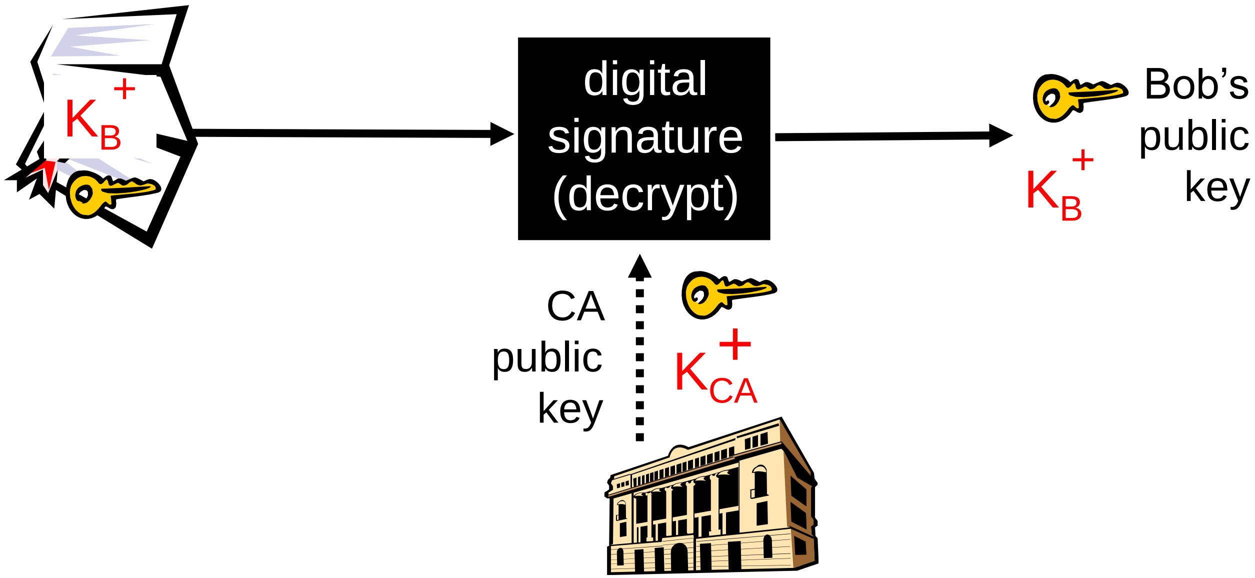
- Certification authority (CA): binds public key to particular entity, E.
- E (person, router) registers its public key with CA.
- E provides “proof of identity” to CA.
- CA creates certificate binding E to its public key.
- Certificate containing E’s public key digitally signed by CA – CA says “this is E’s public key”


Bob’s public key
K_B^+
Bob’s identifying information
digital signature (encrypt)
CA private key
K_{CA}^-
K_B^+
certificate for Bob’s public key, signed by CA

STALLINGS, W. 2022. *Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition*, Pearson.

Certification Authorities (CA)

- When Alice wants Bob’s public key:
- Gets Bob’s certificate (Bob or elsewhere).
- Apply CA’s public key to Bob’s certificate, get Bob’s public key



STALLINGS, W. 2022. *Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition*, Pearson.

Checkpoint Summary

- Key exchange is a critical process in secure communication, ensuring the safe exchange of cryptographic keys.
- TTP, KDC and DH schemes are used to share the keys over insure channels.
- Asymmetric encryption involves public and private keys for secure data transmission and authentication.
- It is often used in key exchange to securely transmit symmetric session keys.

Network Security and Cryptography

Topic 3: Cryptographic Techniques

Lecture 2

Message Authentication Code and Hash Function

Message Authentication

Message authentication is concerned with:

- Protecting the integrity of a message
- Validating identity of originator
- Non-repudiation of origin (dispute resolution)

Message Security Requirements

- Disclosure
- Traffic analyses
- Masquerade
- Content modification
- Sequence modification
- Timing modification
- Source repudiation
- Destination repudiation

Authentication Functions

Any message authentication or digital signature mechanism has two levels of functionality.

- At the lower level, there must be some sort of function that produces an authenticator: a value to be used to authenticate a message.
- This lower-level function is then used as a primitive in a higher-level authentication protocol that enables a receiver to verify the authenticity of a message.

Authentication Functions

- Types of functions that may be used to produce an authenticator are grouped into three classes, as follows:
- Message encryption: The ciphertext of the entire message serves as its authenticator
- Message authentication code (MAC): A function of the message and a secret key that produces a fixed-length value that serves as the authenticator
- Hash function: A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator

Message Authentication Using Encryption

Symmetric Message Encryption

- If symmetric encryption is used, then:
  - ✓ Receiver know sender must have created it
  - ✓ Since only sender and receiver know key used
  - ✓ Know content cannot have been altered if message has suitable structure, redundancy or a suitable checksum to detect any changes

Message Authentication Using Encryption

Asymmetric Message Encryption

- If asymmetric encryption is used, then:
  - ✓ Encryption provides no confidence of sender, since anyone potentially knows public-key.
  - ✓ However, if sender signs message using their private-key then encrypts with recipient's public key have both secrecy and authentication.
  - ✓ Need to recognize corrupted messages but at cost of two public-key uses on message.

Message Authentication Using Encryption

Asymmetric Message Encryption

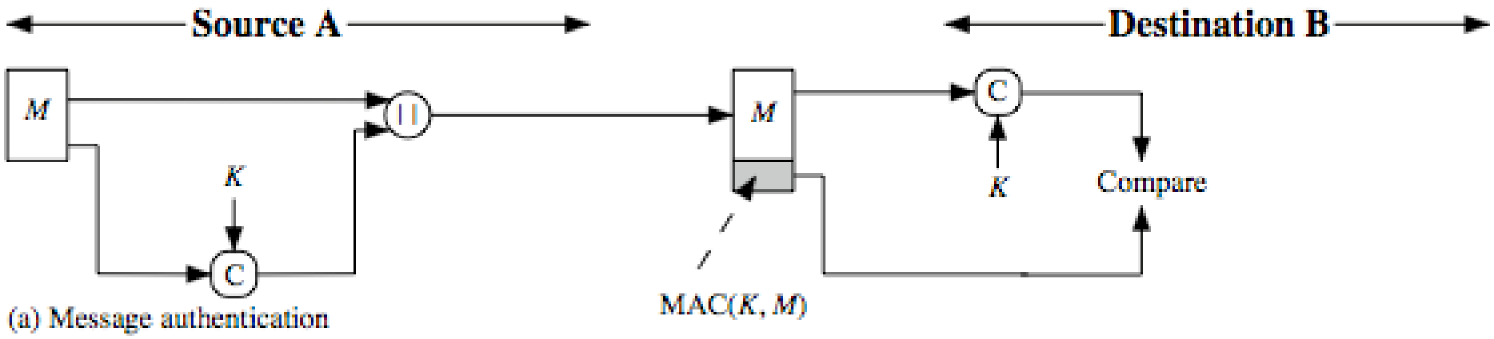
- If asymmetric encryption is used, then:
  - ✓ Every time you encrypt, size expands due to padding.
  - ✓ Signing (by encryption) then encrypting, the size is more than doubled!

Message Authentication Code (MAC)

- Generated by an algorithm that creates a small fixed-sized block
  - ✓ depending on both message and secret key
  - ✓ like encryption though need not be reversible
- Appended to message as a **signature**
- Receiver performs same computation on message and checks it matches the MAC
- Provides assurance that message is unaltered and comes from sender

Message Authentication Code (MAC)

- A small fixed-sized block of data
  - ✓ Generated from message + secret key
  - ✓ MAC = C(K,M)
  - ✓ Appended to message when sent



STALLINGS, W. 2022. *Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition*, Pearson.

Message Authentication Code (MAC)

- As shown the MAC provides authentication

- Can also use encryption for secrecy
  - ✓ Generally, use separate keys for each
  - ✓ Can compute MAC either before or after encryption
  - ✓ Is generally regarded as better done before

Message Authentication Code (MAC)

Why use a MAC?

- Sometimes only authentication is needed
- Sometimes need authentication to persist longer than the encryption (e.g., archival use)
- Note that a MAC is not a digital signature
  - ✓ Does NOT provide non-repudiation

MAC Properties

- A MAC is a cryptographic checksum

  MAC = CK(M)

  - ✓ Condenses a variable-length message M
  - ✓ Using a secret key K
  - ✓ To a fixed-sized authenticator
- Is a many-to-one function
  - ✓ Potentially many messages have same MAC
  - ✓ But finding these needs to be very difficult

Requirements for MACs

Need the MAC to satisfy the following:

- Knowing a message and MAC, is infeasible to find another message with same MAC
- MACs should be uniformly distributed
- MAC should depend equally on all bits of the message

Using Symmetric Ciphers for MACs

- Can use any block cipher chaining mode and use final block as a MAC
- Data Authentication Algorithm (DAA) is a widely used MAC based on DES-CBC
  - ✓ using IV=0 and zero-pad of final block
  - ✓ encrypt message using DES in CBC mode
  - ✓ and send just the final block as the MAC
    - or the leftmost M bits (16≤M≤64) of final block
- But final MAC is now too small for security

Hash Functions

- A cryptographic hash function h is a function which takes arbitrary length bit strings as input and produces a fixed length bit string as output, the hash value.
- A cryptographic hash function should be one-way: given any string y from the range of h, it should be computationally infeasible to find any value x in the domain of h such that

$$h(x) = y.$$

- Given a hash function with outputs of n bits, we would like a function for which finding preimages requires $O(2^n)$ time.

Hash Functions

- Condenses arbitrary message to fixed size
- Usually assume that the hash function is public and not keyed
  - ✓ cf. MAC which is keyed

- Hash used to detect changes to message
- Can use in various ways with message
- Most often to create a **digital signature**

Requirements for Hash Functions

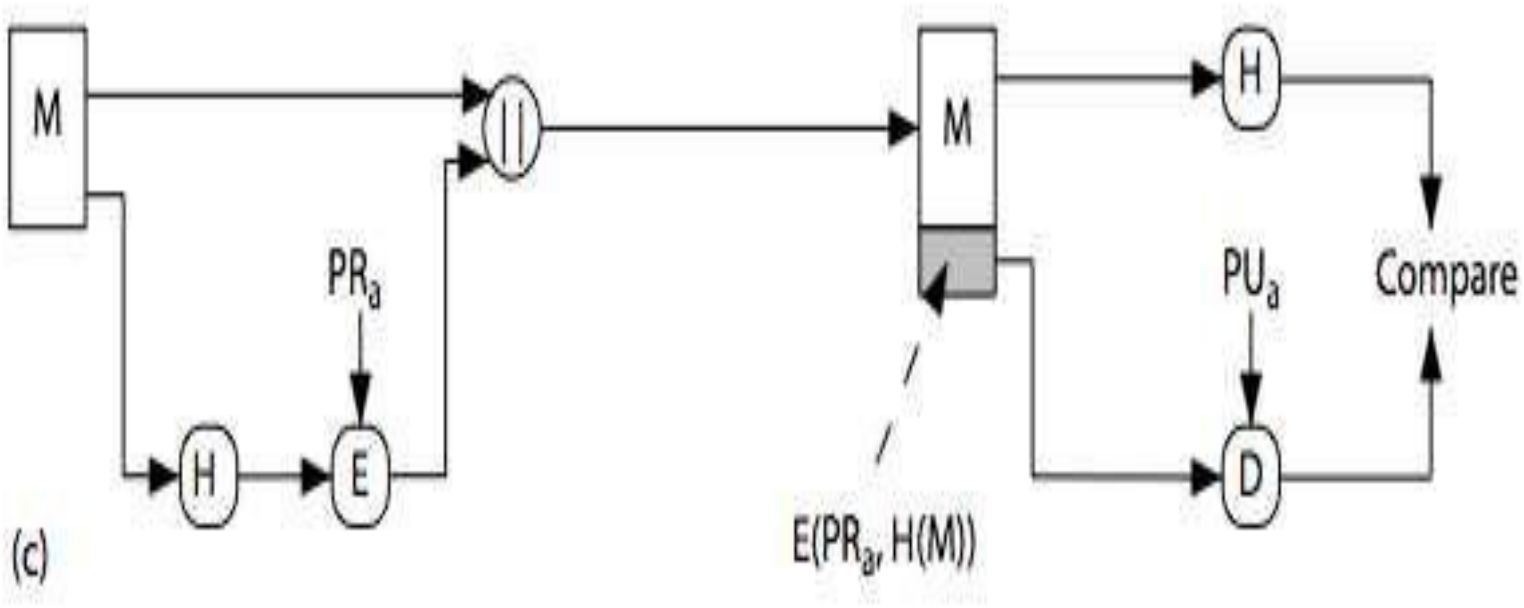
The purpose of a hash function is to produce a "fingerprint" of a file, message, or other block of data. To be useful for message authentication, a hash function `H` must have the following properties:

1. `H` can be applied to a block of data of any size.
2. `H` produces a fixed-length output.
3. `H(x)` is relatively easy to compute for any given `x`, making both hardware and software implementations practical.

Requirements for Hash Functions

4. For any given value h, it is computationally infeasible to find x such that $H(x) = h$. This is sometimes referred to in the literature as the one-way property.
5. For any given block x, it is computationally infeasible to find y x such that $H(y) = H(x)$. This is sometimes referred to as weak collision resistance.
6. It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$. This is sometimes referred to as strong collision resistance

Hash Functions & Digital Signature



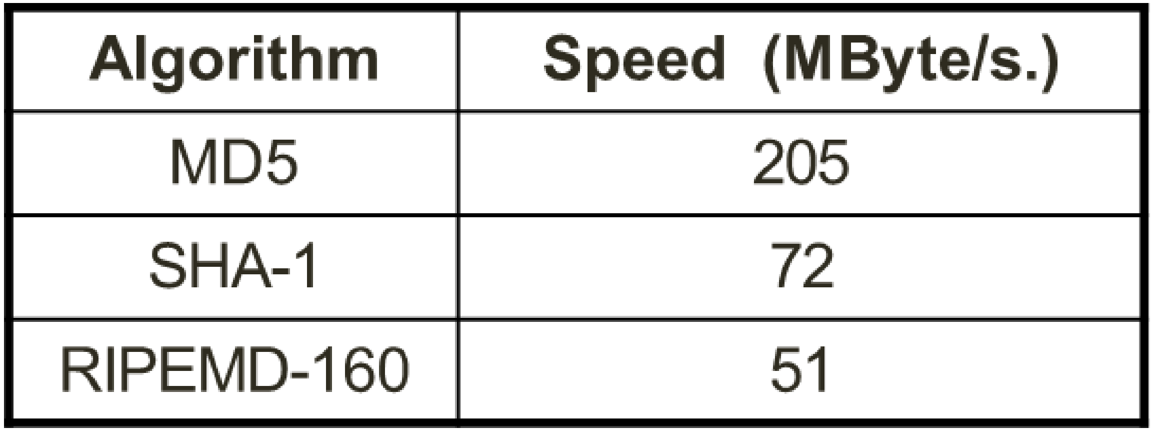
STALLINGS, W. 2022. *Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition*, Pearson.

Birthday Attacks

- Might think a 64-bit hash is secure
  - ✓ But by Birthday Paradox is not
- Birthday attack works thus:
  - ✓ Opponent generates $2^{m/2}$ variations of a valid message all with essentially the same meaning
  - ✓ Opponent also generates $2^{m/2}$ variations of a desired fraudulent message
  - ✓ Two sets of messages are compared to find pair with same hash (probability > 0.5 by birthday paradox)
  - ✓ Have user sign the valid message, then substitute the forgery which will have a valid signature
- Conclusion is that need to use larger MAC/hash

Some Popular Hash Algorithms

- MD5 (Rivest Most popular) 128 bits
- SHA-1 (Secure Hash Algorithm-1 by NIST) 160-bit
- SHA-2 (Family of Hash Algorithms by NIST) 224-512 bit
- RIPEMD-160 (Euro. RIPE project) 160-bit output



Algorithm	Speed (MByte/s.)
MD5	205
SHA-1	72
RIPEMD-160	51

Crypto++ 5.1 benchmarks, 2.1 GHz P4

Usage of Hash Algorithms

- Commit to message by disclosing hash of message, later showing the message
- If collision resistant, you cannot cheat (change message).
- Verify integrity of downloaded files.
- Digital signatures.
- SSL/TLS for integrity protection.
- Storing passwords in operating systems and web servers.

Topic Summary

- Key exchange is a critical process in secure communication, ensuring the safe exchange of cryptographic keys.
- Asymmetric encryption involves public and private keys for secure data transmission and authentication.
- Message authentication code (MAC): A function of the message and a secret key that produces a fixed-length value that serves as the authenticator
- Hash function: A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator
- Hash function is used for **digital signatures**

Next Topic 4: Operating System Security and Vulnerabilities

- Operating System Security basics
- User Authentication
- Unix Access Control

References

- CHARLES J. B., Christopher G., Philip C., Donald S. 2018. Cybersecurity Essentials, John Wiley & Sons, Inc.
- CIAMPA, M. (2012). Security+ guide to network security fundamentals. Cengage Learning.
- HOFFMAN, A. 2020. Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly.
- OZKAYA, E. 2019. Cybersecurity: The Beginner's Guide. Packet Publishing Ltd.
- STALLINGS, W. 2022. Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition, Pearson.

NCC education ® Awarding Great British Qualifications

Topic 3 – Cryptographic Techniques

Any Questions?