School of InfoComm Technology ict Taking IT Higher

NGEE ANN POLYTECHNIC

1

CRYPTOGRAPHY (CTG)

Diploma in Cybersecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `21/`22 – Semester 2

WEEK 4.1

ASYMMETRIC KEY CRYPTOSYSTEM

Last Updated: 15/10/2021

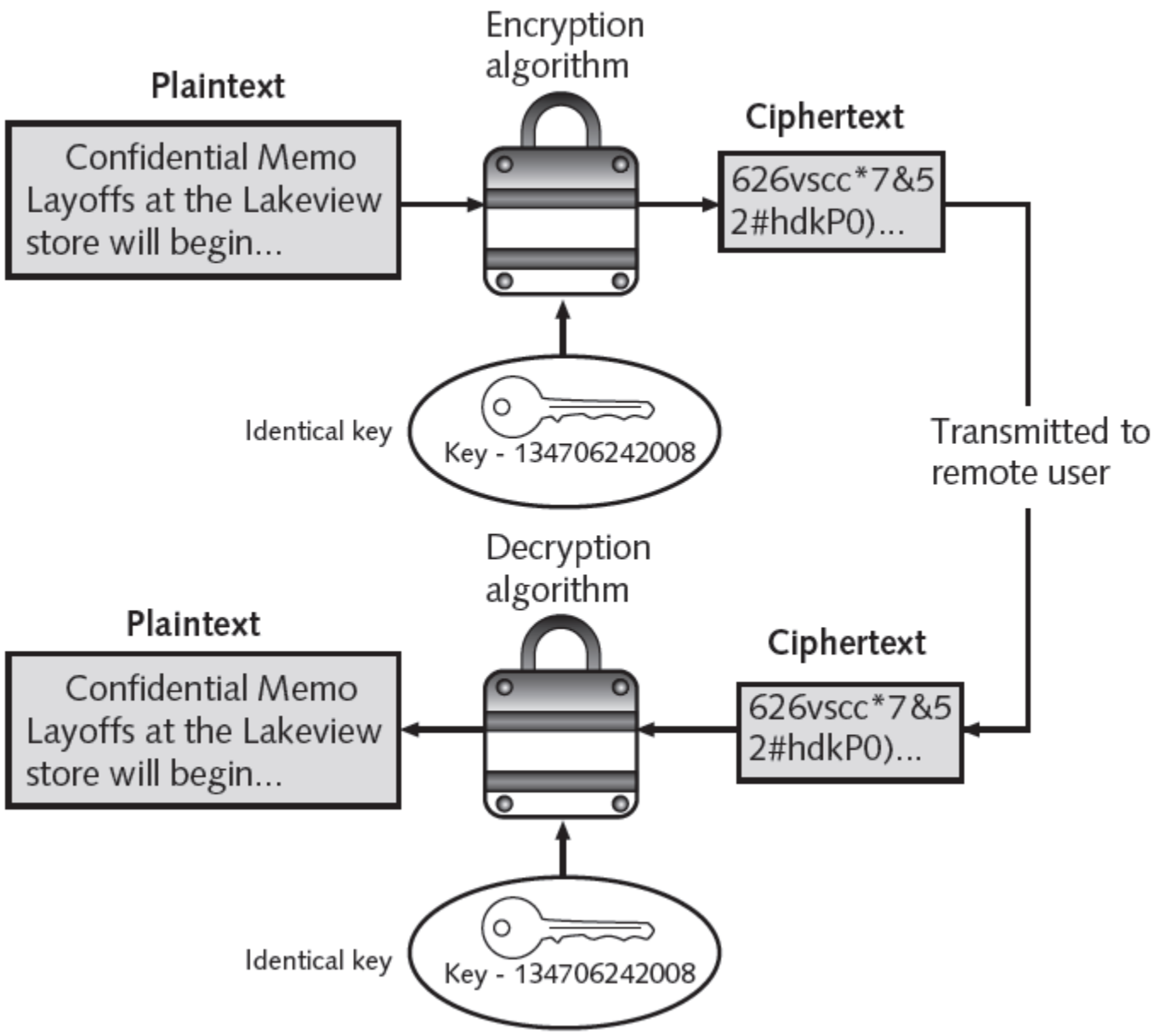
Contents

Recap – Week 3

- Symmetric Key Cryptosystem
- Advantages and Disadvantages of Symmetric Key Cryptosystem
- Symmetric Key Cryptosystem and Goals of Cryptography

Symmetric Key Cryptosystem

Same shared key used to encrypt and decrypt data



(Source: SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS 4th Edition – Mark Ciampa - Cengage Learning)

Advantages and Disadvantages of Symmetric Key Cryptosystem

- Advantages
  - Extremely secure
  - Relatively fast
    - Due to simple substitution, permutation (transposition), and modular arithmetic operations
- Disadvantages
  - Key distribution
    - Requires a secure communication channel to share key between parties
  - Key management
    - Each party have to maintain a unique shared key with every other communicating party
    - If “n” is the number of parties in a group, who want to use symmetric key cryptosystem
      - Then the total number of keys required for the group would be: n x (n -1) / 2

Symmetric Key Cryptosystem and Goals of Cryptography

- Discuss why Symmetric Key Cryptosystem does/doesn't satisfy the following goals of cryptography?

Goals of Cryptography	Symmetric Key Cryptosystems (Yes/No)
Confidentiality	??
Integrity	??
Availability	??
Authentication	??
Non-Repudiation	??

Why Asymmetric Key Cryptosystem?

Why Asymmetric Key Cryptosystem?

- Due to disadvantages of symmetric key cryptosystem and in order to satisfy other goals of cryptography
- In 1976 an asymmetric-key cryptosystem was published
  - Whitfield Diffie, Martin Hellman, and Ralph Merkle
  - Diffie–Hellman–Merkle key exchange
- In 1977 another asymmetric-key cryptosystem was independently invented
  - Ron Rivest, Adi Shamir and Leonard Adleman
  - RSA Cryptosystem (from their initials)

9

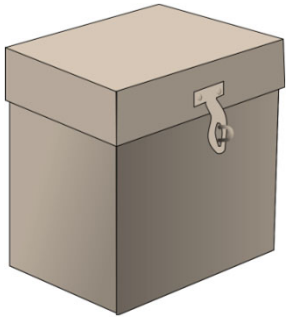
Asymmetric Key Cryptosystem

Concept of Asymmetric Key Cryptosystem

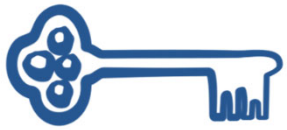
Discuss how Alice and Bob can securely send each other letters?

Alice

Alice's Letter to Bob

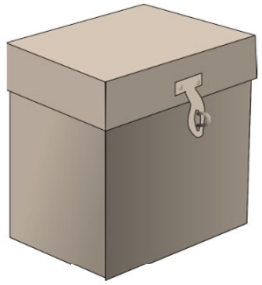


Alice's Padlock



Alice's Key

Bob



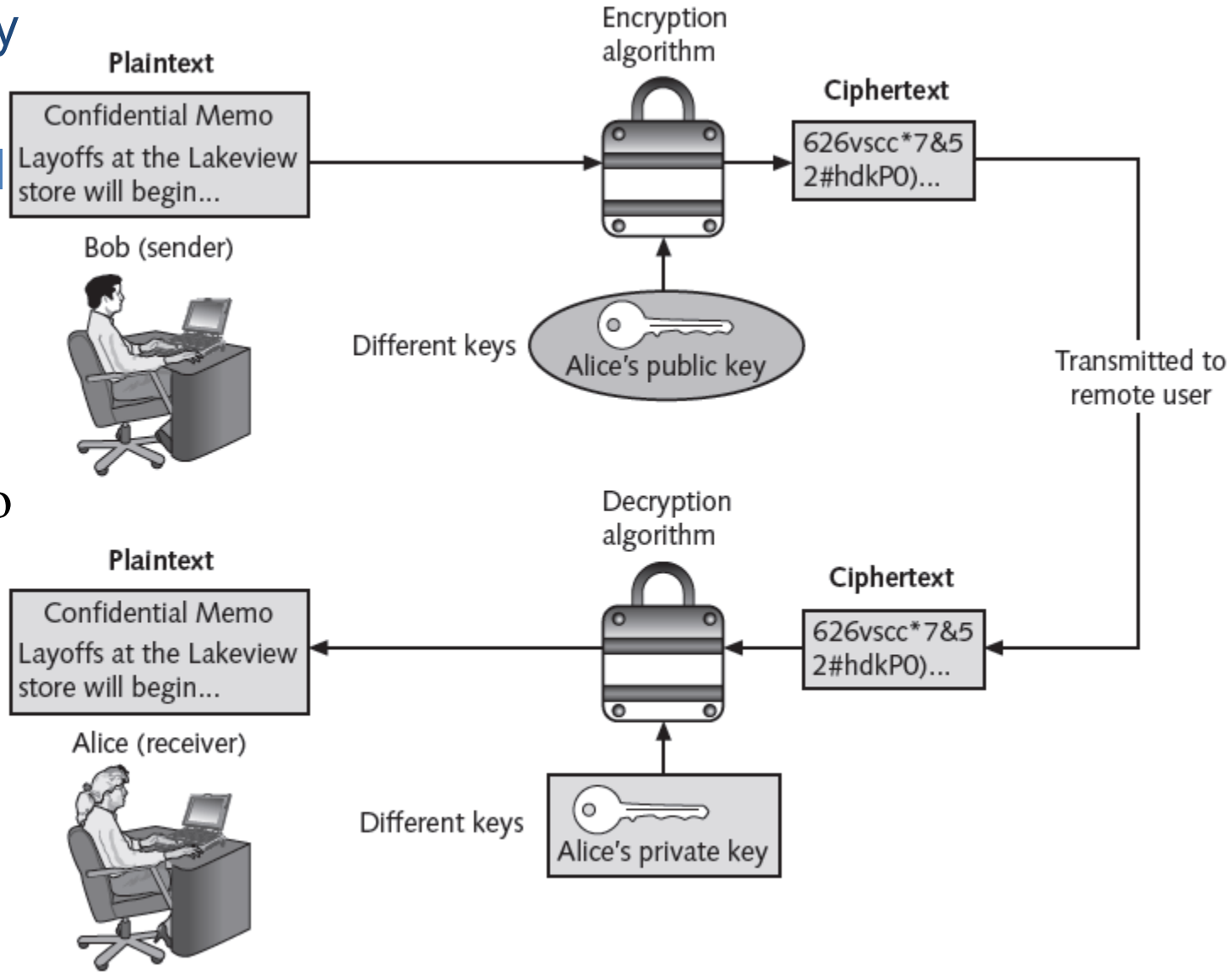
Bob's Letter to Alice

Bob's Padlock

Bob's Key

Asymmetric Key Cryptosystem

Public-key to encrypt and Private-key to decrypt data



(Source: SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS 4th Edition – Mark Ciampa - Cengage Learning)

Other Names

- Symmetric Key Cryptosystem also known as
  - Private/Secret-key cryptosystem
  - Private/Secret-key cryptography

- Asymmetric Key Cryptosystem also known as
  - Public-key cryptosystem
  - Public-key cryptography

Popular Asymmetric Key Cryptosystems

- RSA
  - Published in 1977 and patented by MIT in 1983
  - Most common asymmetric cryptography algorithm
  - Uses two large prime numbers
- Elliptic curve cryptography (ECC)
  - Users share one elliptic curve and one point on the curve
  - Uses less computing power than prime number-based asymmetric cryptography
    - Key sizes are smaller

Kid RSA

Asymmetric Key Cryptosystem – Kid-RSA

- Kid-RSA is an asymmetric cryptosystem similar to RSA, but is simpler than RSA.
- proposed by Neal Koblitz for teaching cryptography without using advanced mathematics
- Kid-RSA uses public-private key pair for encryption and decryption

Asymmetric Key Cryptosystem – Kid-RSA

- Alice chooses 4 random integers
  - a, b, a1, b1
- Then, Alice computes the following: M, e, d, n
  - M = a * b -1
  - e = a1 * M + a
  - d = b1 * M + b
  - n = ((e * d) – 1) / M
- Alice's public-key = (n, e)
- Alice's Private-key = d

Asymmetric Key Cryptosystem – Kid-RSA

- Let: a = 9, b = 11, a1 = 5, b1 = 8;
- Therefore:

M	**(*a* * *b*) - 1**	**(9 * 11) -1**	**98**
e	(*a1* * *M*) + a	(5 * 98) + 9	499
d	(*b1* * *M*) + b	(8 * 98) + 11	795
n	((*e* * *d*) - 1)/M	((499 * 795) -1) / 98	4048

- The plaint text has to be a number in the range of 0 to n-1.
- Let the message be PT = 538.
- Encryption
  - CT = PT * e (mod n) = 499 * 538 (mod 4048) = 268462 (mod 4048) = 1294
- Decryption
  - PT = CT * d (mod n) = 1294 * 795 (mod 4048) = 1028730 (mod 4048) = 538

Source: http://www.cs.uri.edu/cryptography/publickeykidkrypto.htm

Kid-RSA Exercise

- Exercise
  - Let: a = 3, b = 4, a1 = 5, b1 = 6;
  - CT = 161
  - PT = ???

Asymmetric Key Cryptosystem and Goals of Cryptography

Asymmetric Key Cryptosystem and Goals of Cryptography

- Discuss why Asymmetric Key Cryptosystem does/doesn't satisfy the following goals of cryptography?

Goals of Cryptography	Asymmetric Key Cryptosystems
Confidentiality	??
Integrity	??
Availability	??
Authentication	??
Non-Repudiation	??

Asymmetric Key Cryptosystem – Satisfies Confidentiality

- Alice's public-private key pair
  - Public-key and Private-key are two mathematically related keys
  - Public-key is shared publicly
    - Alice makes her public-key, publicly available to all.
    - Whoever, wants to send Alice a secure message, would have to encrypt the message using her public key.
  - Private-key is kept secret/private with Alice at all times
    - Alice is the only one who can decrypt the cipher messages sent to her using her private-key.
- Charlie may capture the cipher messages for Alice, but he cannot decrypt them as he does not have Alice's private-key.
- It is impossible for Charlie to generate Alice's private-key based on (the publicly available) Alice's public-key.

Asymmetric Key Cryptosystem – Satisfies Authenticity and Non-Repudiation

- Alice's public-private key pair are two mathematically related keys
  - Authenticity and Non-Repudiation
    - When Alice wants to prove that a message is from her.
    - Alice encrypts that message with her private-key.
    - Whoever wants to verify the message, would be able to decrypt the message ONLY with Alice's public-key.
    - Since the message could ONLY be decrypted by Alice's public-key, and also Alice ALONE holds the private-key, it proves that the message came from Alice.
- Discuss:
  - Charlie can also decrypt the cipher message in this case, because he too know Alice's public Key.
  - So how to keep this cipher message secure from Charlie?

Asymmetric Key Cryptosystem – Combining Confidentiality, Authentication, and Non-Repudiation

- Alice wants to achieve both the following requirements in one go:
  - Confidentiality
    - Alice wants to send a secure message to Bob
  - Authentication and Non-Repudiation
    - Alice wants to prove to Bob that she indeed sent the message
- Discuss how Alice can do the above using Asymmetric Key Cryptosystem

Asymmetric Key Cryptosystem – Combining Confidentiality, Authentication, and Non-Repudiation

- Type your answer here

Alice encrypts the msg with her private key then crypts it agn w Bob's public key so even if Charlie gets the msg, he does not have Bob's private key to decrypt the 2nd Encryption which is Bob's public key.

Symmetric vs. Asymmetric

Symmetric vs. Asymmetric

Uses a secret key to encrypt and to decrypt messages.	Uses two keys, one by the sender and one by the receiver to encrypt and to decrypt messages respectively. The two keys are mathematically related.
The secret key cannot be made public and known only to the sender and receiver.	One of the keys, i.e. the public key can be made known to all parties concerned. While the sender keeps the other key, i.e. private key.
Need a secure channel to distribute the key.	Allows public keys to be exchanged out in the open over insecure communication channels.
Perform faster than most public key cryptographic algorithms.	Perform slower than most symmetric cryptographic algorithms.
Number of symmetric keys = N(N-1)/2, where N is the number of users in the group	Number of Asymmetric Keys = 2N, where N is the number of users in the group
Satisfies only Confidentiality, Availability	Satisfies Confidentiality, Availability, Authentication, Non-Repudiation

Summary

Summary

Component	You learnt
Knowledge	Why Asymmetric Key Cryptosystem? Asymmetric Key Cryptosystem Other names of asymmetric key crypto Kid-RSA Popular Asymmetric Key Cryptosystems: RSA, ECC Symmetric vs. Asymmetric
Thinking	Symmetric Key Cryptosystem and Goals of Cryptography Concept of Asymmetric Key Cryptosystem Asymmetric Key Cryptosystem and Goals of Cryptography
Skill	Kid-RSA
Activity	Kid-RSA Symmetric Key Cryptosystem and Goals of Cryptography Concept of Asymmetric Key Cryptosystem Asymmetric Key Cryptosystem and Goals of Cryptography
Feedback	Symmetric Key Cryptosystem and Goals of Cryptography Concept of Asymmetric Key Cryptosystem Asymmetric Key Cryptosystem and Goals of Cryptography