Applied Cryptography

Public Key Cryptography

Learning Objectives

Upon completion of this unit:

- Students will be able to explain how asymmetric (public key) encryption works.
- Students will be able to explain the difference between symmetric and asymmetric encryption and the need for public key cryptography.
- Students will be able to explain the use of key exchange/agreement protocols in cryptography.
- Students will be able to identify commonly used algorithms for asymmetric encryption.
- Students will be able to illustrate how public key encryption works using software such as Kryptos.

Recall: Cryptography

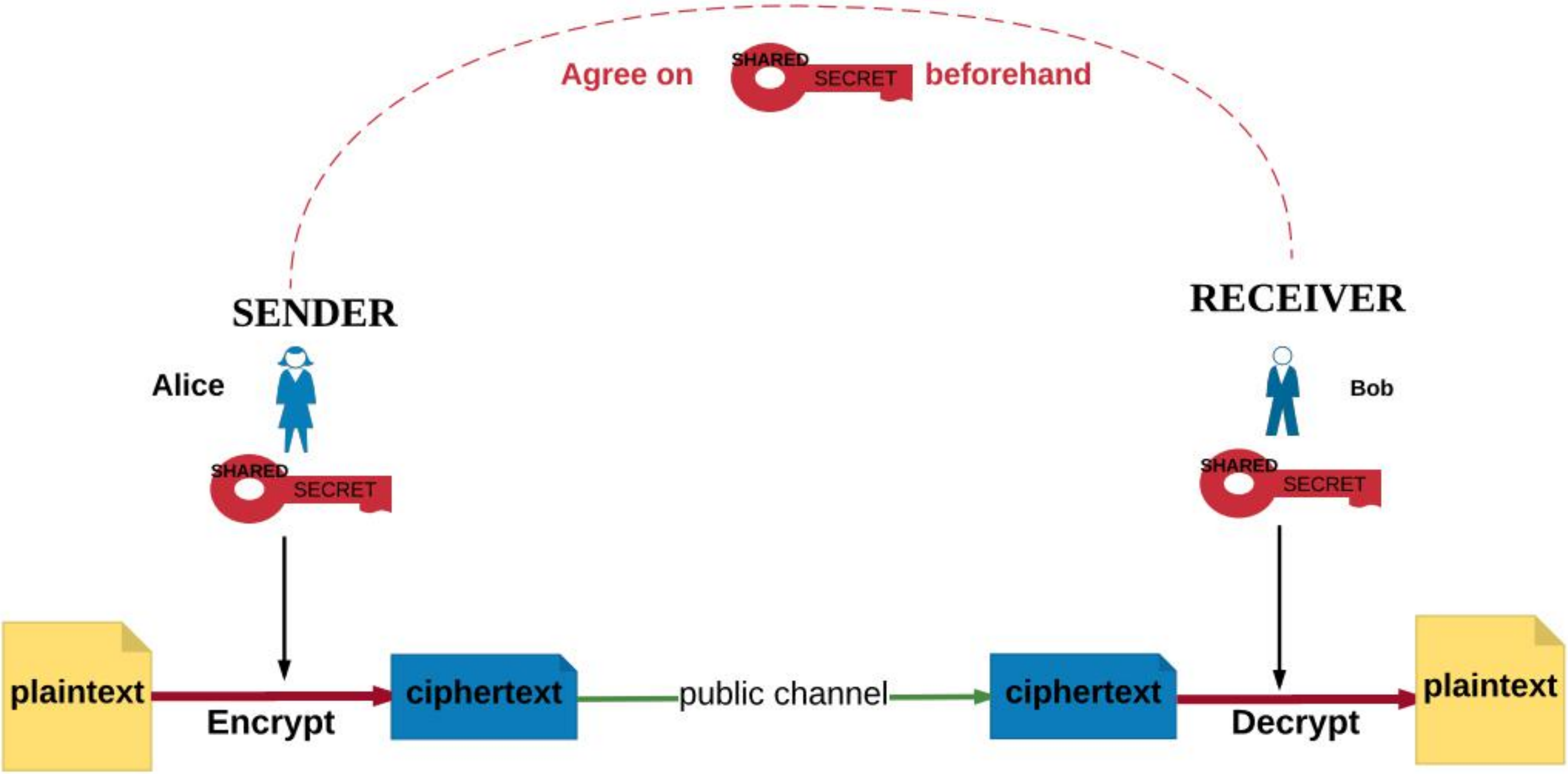
- Cryptography is “the practice and study of techniques for secure communication in the presence of adversaries” (Wikipedia)

- It is the science of designing systems to store and transmit data in a secure way so that it preserves its integrity and is accessible to only those with proper authentication and authorization.

Recall: Cryptography and the Main Tenets of Information Security

- Confidentiality
  - Encryption algorithms
- Integrity
  - Hash functions
- Authenticity
  - Digital signatures, digital certificates
- Non-repudiation
  - Digital signatures, digital certificates

Recall: Symmetric Key Cryptography



“Symmetric Encryption" by Yesem Kurt-Peker licensed under CC BY 4.0

Recall Problem of Key Distribution and Management

- Modern symmetric key algorithms are great! They are fast and secure when implemented correctly and keys are chosen properly.

- Problem: How to get the keys to the two parties?
  - Need a secure channel – a channel that makes it very difficult for the adversary to access the actual plaintext that is being transmitted.
  - But the Internet is not secure!

- **Solution:** Public Key Cryptography

Public Key Cryptography

- Each user has a public and a private key.
- Public keys are published.
- Private keys are secret. (Only **one** party, the owner, knows the private key, **NOT** both parties!)

Solutions for Key Distribution

1. Public Key Encryption:

   Encrypt the shared secret key for symmetric ciphers using asymmetric (public key) encryption and send over the (not secure) channel.

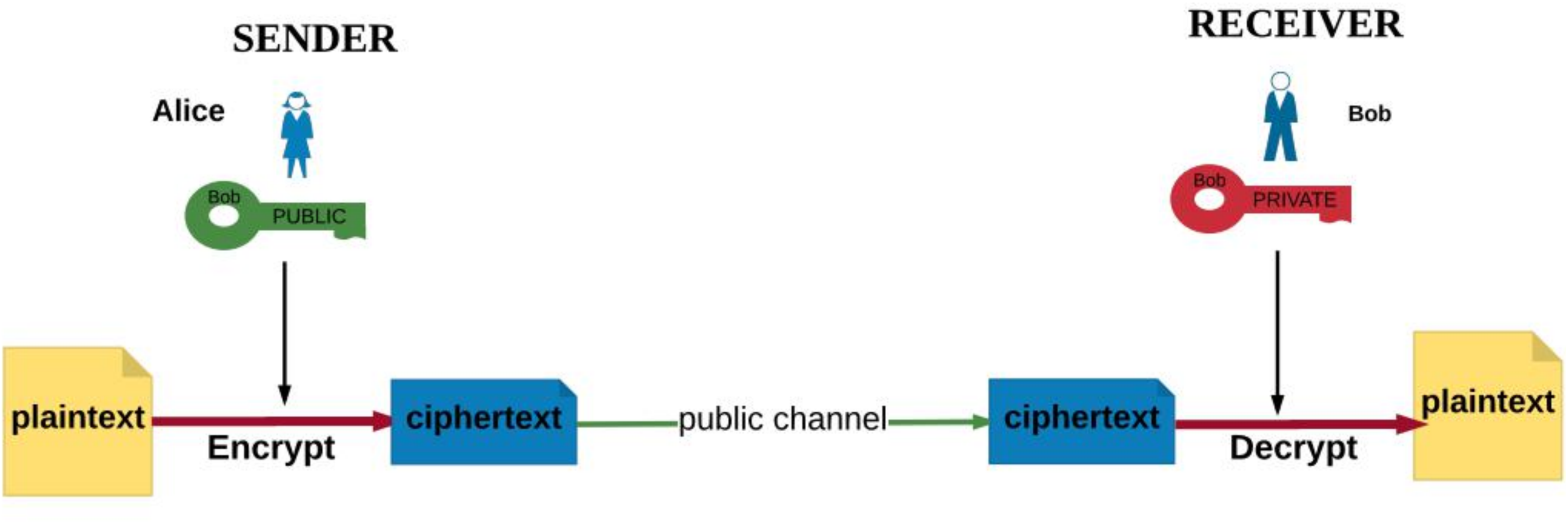
2. Key Agreement Algorithms:

   Use public and private keys to agree on a key without exchanging any private information.

Solution 1. Asymmetric Encryption/Decryption

- If Alice wants to send Bob a confidential message, she gets **Bob's** public key.
- She encrypts her message to Bob using **Bob**'s public key and sends it to Bob (possibly over the Internet).
- Bob, upon receipt of the encrypted message from Alice, uses **his** private key to decrypt the message.
- Because only Bob knows his private key, only he can decrypt the message and read it!

Asymmetric Encryption



“Asymmetric Encryption" by Yesem Kurt-Peker licensed under CC BY 4.0

Note that no communication is necessary beforehand to agree on a shared secret key.

Advantage of Asymmetric Encryption

- With asymmetric encryption, users do not have to share a secret value that they have to communicate or agree on beforehand or over a public channel.

- Public keys are published and available to everyone in the system.

- **NOTE:** Private keys should NOT be shared!

Examples of Asymmetric Encryption Algorithms

- RSA Encryption
  - Developed by Rivest, Shamir, Adleman (scientists at Berkley) in 1976
  - Included in the cipher suite for key agreement/exchange in TLS/SSL (Transport Layer Security/Secure Socket Layer)
- Elliptic Curve Encryption
  - Suggested independently by N. Koblitz and V. Miller in 1985
  - Included in the cipher suite for key agreement / exchange in TLS/SSL (https://en.wikipedia.org/wiki/Cipher_suite)
  - Also included in Bluetooth Low Energy (LE) protocols

A Glimpse of the RSA Encryption

- **Key generation by Bob:**
  - Select p, q $\quad$ p and q both prime, p ≠q
  - Calculate $\quad n = pxq$
  - Calculate $\varphi(n) = (p-1)(q-1)$ (Euler's phi function)
  - Select e $\quad 1 < e \ < \varphi(n),\ \gcd\big(e, \varphi(n)\big) = 1$
  - Calculate d $\quad d = e^{-1}\, mod\ \varphi(n)$
  - Public key (e, n) $\quad$ Private key (d, n)
- **Encryption by Alice (of a message for Bob)**
  - Plaintext (message) $\quad M < n$
  - Ciphertext $\quad C = \ M^e\ mod\ n$
- **Decryption by Bob (of the message from Alice)**
  - Ciphertext $\quad C$
  - Plaintext $\quad M = \ C^d\ mod\ n$

One Problem: Authentication

- How does Bob know that the message is indeed from Alice?
- Someone else might have used Bob’s public key, sent him the message, and claimed he/she was Alice!
- Solution: Digital signatures and certificates

Solution 2. Key Agreement (Exchange) Protocols

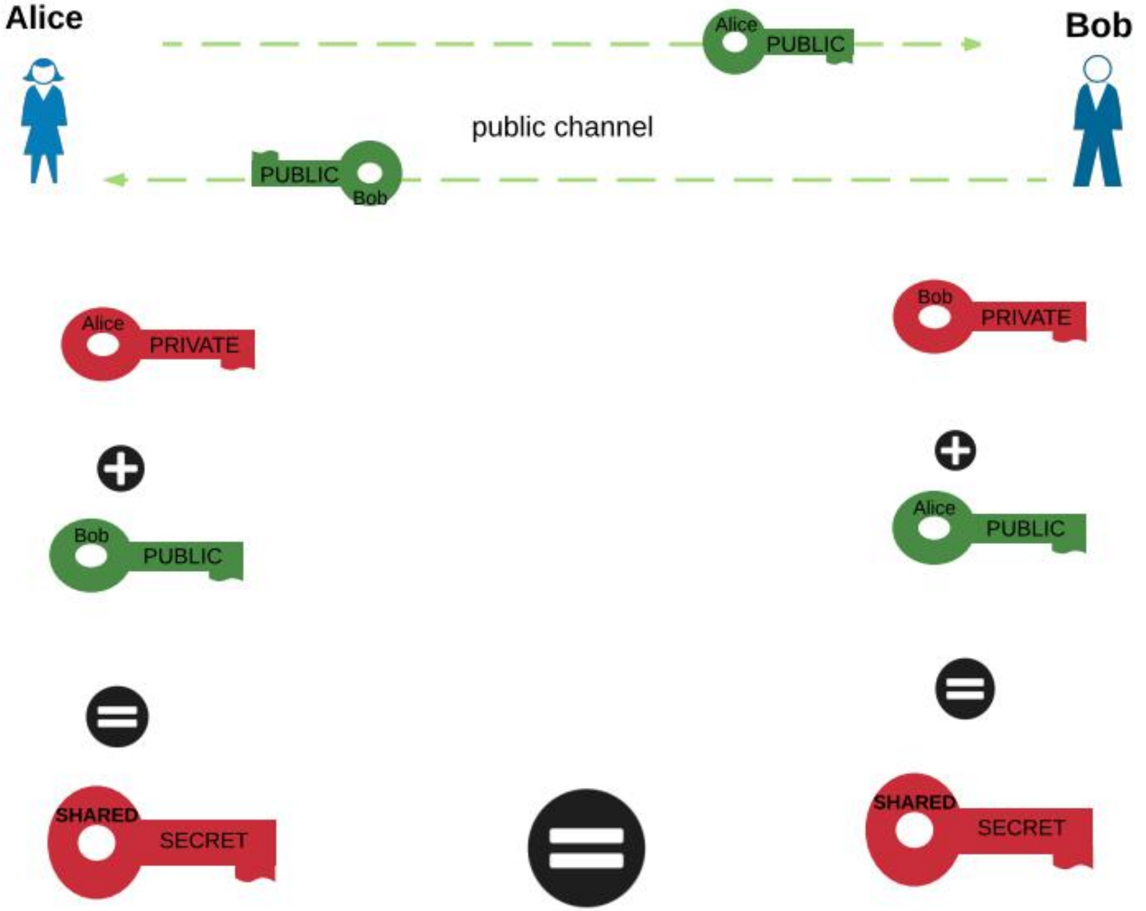
- Public Key Cryptography gives us another way to communicate privately without having to share secret information prior to the communication.

- Purpose is to enable two users to securely agree on a key that can then be used for subsequent symmetric encryption of messages.

Key Agreement Protocols

- Alice and Bob both have public and private keys.
- These keys are chosen so that Alice and Bob can compute the same number using their **own private key** and the **other's public key**.
- This key that they compute is very hard to find without the knowledge of one of the private keys or with the knowledge of both the public keys.

Key Agreement



“Key Agreement" by Yesem Kurt-Peker licensed under CC BY 4.0

Examples of Key Agreement Schemes

- Diffie-Hellman Key Agreement (DH)
  - **First public key algorithm (1976)**
  - Developed by Diffie and Hellman and Merkle independently
  - Included in the cipher suite for key agreement/exchange in TLS/SSL and Bluetooth Low Energy (LE) protocols

- Elliptic Curve Diffie-Hellman Key Agreement (1985)
  - Same idea as DH but works on elliptic curves
  - Included in the cipher suite for key agreement/exchange in TLS/SSL and Bluetooth (LE) protocols

Use of Key Agreement Protocols

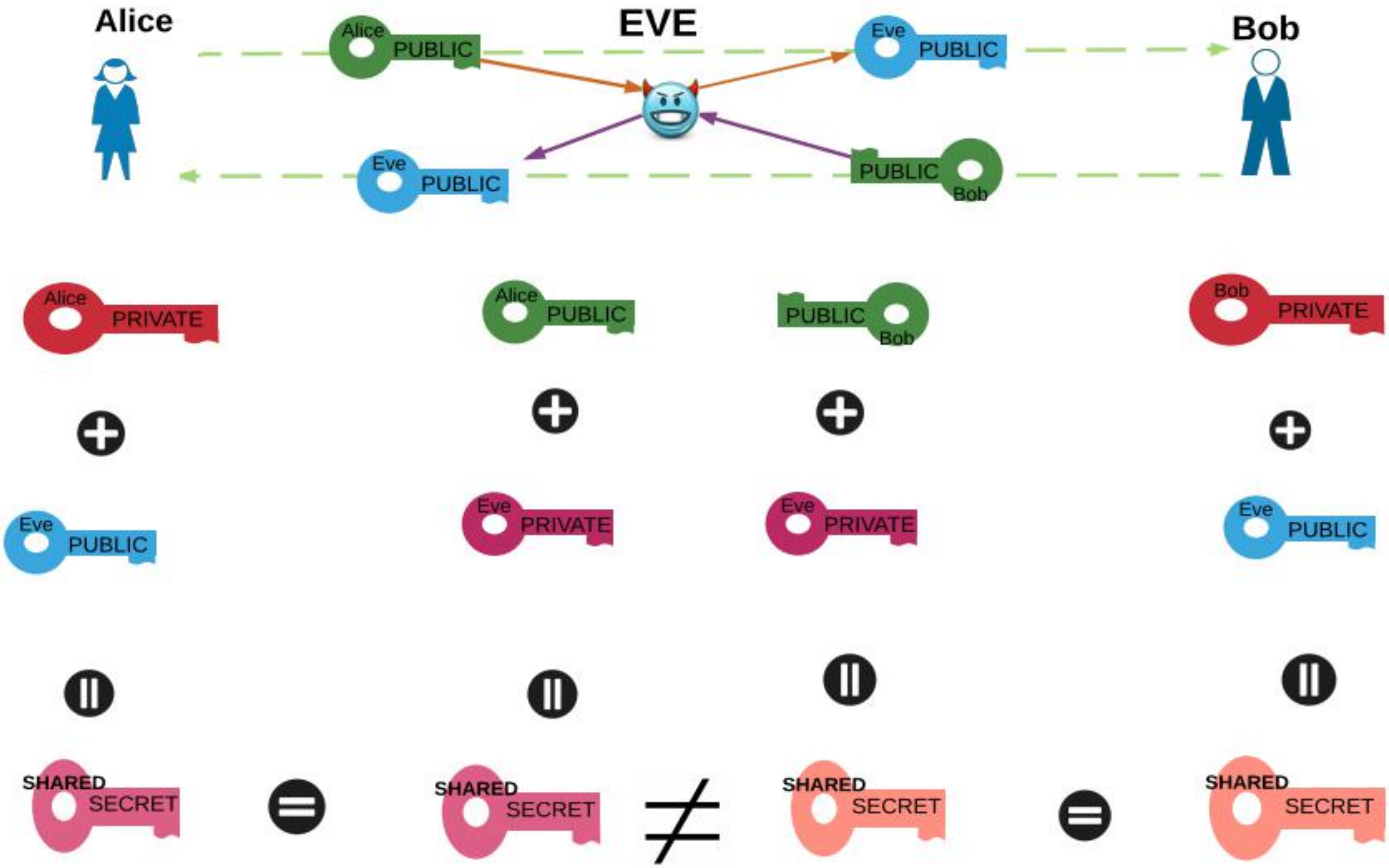
- Users could create random private/public keys **each** time they communicate

  OR

- Users could create private and public keys and **publish** the public key

- **Problem:** Vulnerable to Man-in-the-Middle-Attack

Man in the Middle (MITM) Attack



“Man in the Middle Attack" by Yesem Kurt-Peker licensed under CC BY 4.0

Another Problem: Integrity

- How does Bob know that the message was not altered on the way (in transit)?
  - Even if Bob is able to authenticate that the message is from Alice, it may be that someone altered the message on the way and then put the signature back on it. How can he avoid this?

- Solution: Hash functions

Catalyzing Computing and Cybersecurity in Community Colleges

is funded by a National Science Foundation grant and
is located at Whatcom Community College

237 West Kellogg Road
Bellingham, WA 98226

www.C5colleges.org