Asymmetric Encryption

- CEG 6430/4430 Cyber Network Security
- Junjie Zhang
- junjie.zhang@wright.edu
- Wright State University

Encryption and Decryption

- plaintext: m
- secret: k
- ciphertext: c
- encryption: $c = enc(m, k_{enc})$
- decryption: $m = dec(c, k_{dec})$

Symmetric and Asymmetric Encryption

Symmetric Encryption

- Use the same key for both encryption and decryption.
- $k_{enc} == k_{dec}$

Asymmetric Encryption

- Use different keys for both encryption and decryption.
- $k_{enc} \neq k_{dec}$

Public Key and Private Key

Asymmetric Encryption:

$$c = enc(m, s)$$
$$m = dec(c, k)$$

(s, k) forms a public-private key pair. One is kept as secret and another one is shared with the public.

Some Asymmetric Encryption Algorithms

- RSA
- Diffie-Hellman, ECDSA, ECDH
  - However, they are more likely to be considered as *key exchange algorithms*.

RSA

- Rivest-Shamir-Adleman
- Published in 1977

RSA

RSA - An Example

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)

RSA - An Example

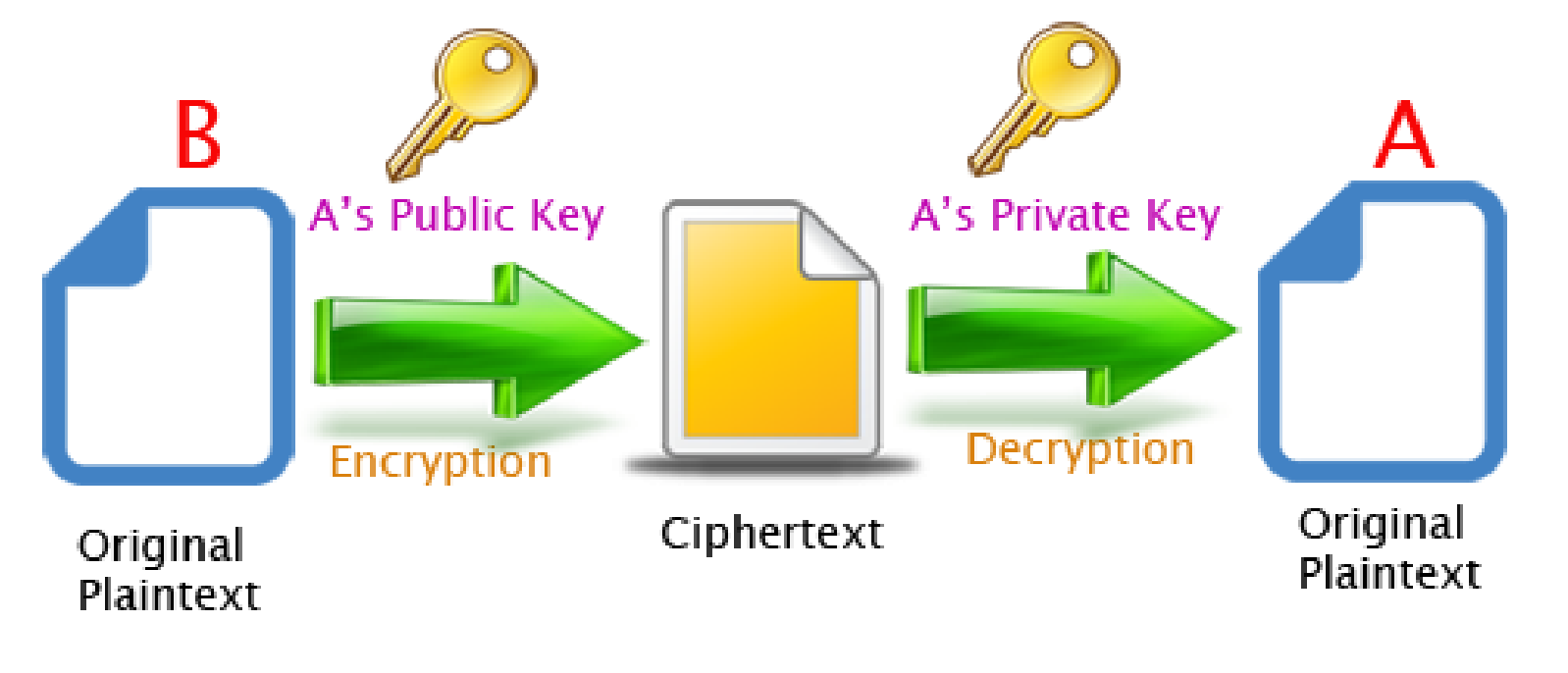
- The encryption of m = 2 is c = 27 % 33 = 29
- The decryption of c = 29 is m = 293 % 33 = 2

Applications of RSA

RSA can be used for

- Encryption
- Signature

Use RSA to Encrypt Data



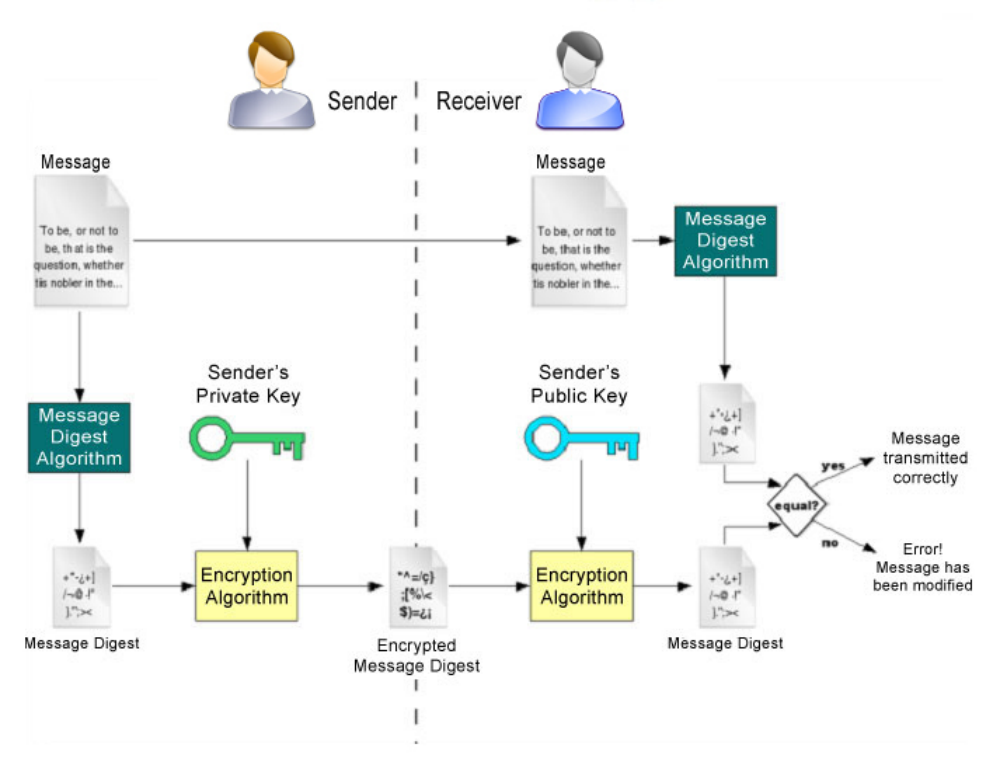
Use RSA to Encrypt Data

- However, RSA is rarely used to encrypt actual data in practice, especially when the size of the data is large. This is because of RSA's high computational cost.
- But, **RSA can be used to send the ciphertext of a symmetric key, which has a small size**. (see the next page).

Use RSA to Share A Symmetric-Encryption Key

- The sender randomly generates a symmetric secret key.
- The sender encrypts this secret key using the reciever public key.
- The receiever decrypts the ciphertext using its private key.
- Bulk data can not be encrypted using the symmetric secret key (i.e., using a mode of operation).

Use RSA for Digital Signature



Symmetric vs Asymmetric Encryption

Symmetric Encryption

- Pros: more computationally efficient.
- Pros: works with encryption modes to encrypt large messages.
- Cons: parties need to share the key first.

Asymmetric Encryption

- Pros: easy to share keys.
- Cons: less computationally efficient.

Symmetric vs Asymmetric Encryption

Asymmetric Encryption -> Typically Used for Limited Data

Symmetric Encryption -> Typically Used for Bulk Data