CRYPTOGRAPHY

PRESENTED BY

SHILPA KHURANA

A.P CSE DEPT.

Basic Terms in Cryptography

Plain text – A message in its natural format readable by an attacker.

Cipher text – A message altered to be unreadable by anyone except the intended recipients.

Key – Sequence that controls the operation and behavior of the cryptographic algorithm.

Cryptosystem – The combination of algorithm, key, and key management functions used to perform cryptographic operations.

Cryptanalysis

- Definition:-

  The art or process of deciphering coded messages without being told the key.

  The attacker or the intruder does not have any knowledge of the key or the algorithm.

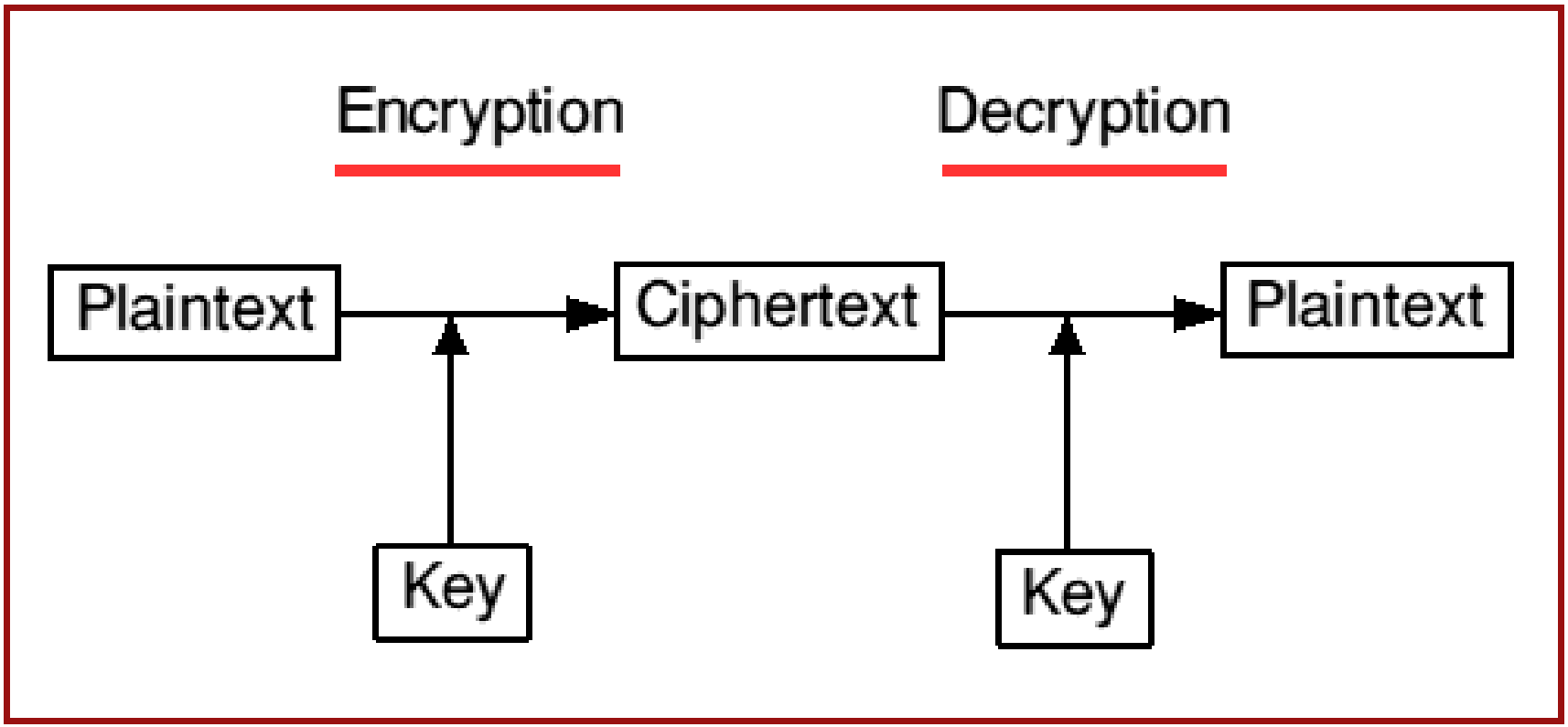
  The attacker can use various methods and try to break the code.

Public Key

- A cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key).

Private Key

- A Private key is an encryption /decryption key known only to the party or parties that exchange secret messages. In cryptography, this key would be shared by the communicators so that each could encrypt and decrypt message.


Encryption
Decryption
Plaintext
Ciphertext
Plaintext
Key
Key

Cryptography Methods

- **Symmetric**
  - Same key for encryption and decryption
  - Key distribution problem
- **Asymmetric**
  - Mathematically related key pairs for encryption and decryption
  - Public and private keys

Introduction to RSA Algorithm

RSA was first described in 1977 by **Ron Rivest**, Adi **Shamir** and Leonard **Adleman** of the Massachusetts Institute of Technology.

Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private.

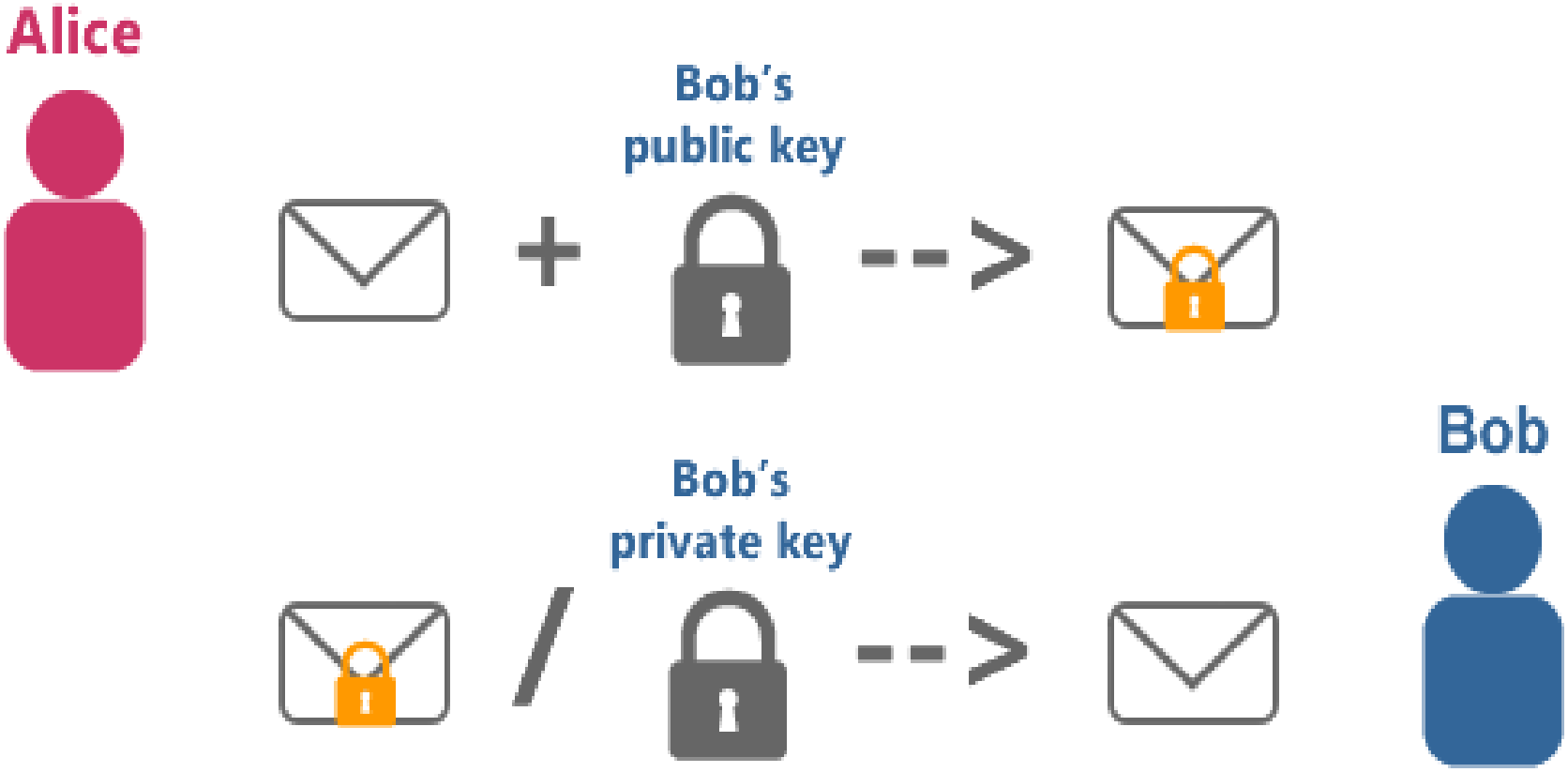
The public key can be shared with everyone, whereas the private key must be kept secret.

- In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it.

- This is one reason why RSA has become the most widely used asymmetric algorithm.

- It provides a method of assuring the confidentiality, integrity, and authenticity of electronic communications and data storage.

Working of RSA



RSA Algorithm

1. **Choose 2 distinct prime numbers.**
   p = 3 and q = 11.

2. **Compute n = p * q = 3 * 11 = 33**

3. **Compute the Totient function**
   φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20

4. **Choose e such that 1 < e < φ(n) and e and n are co-prime. Let e = 7**

5. **Compute a value for d such that (d * e) % φ(n) = 1.**
   Lets say d = 3
   i.e. [(3 * 7) % 20 = 1]

6. Public key is (e, n) => (7, 33)
   Private key is (d, n) => (3, 33)

7. For a plain text message *m*, the encryption function is
   $c(m) = m^e \bmod \varphi(n)$.

8. Assuming m=2,

   The encryption of *m = 2* is
   $c(m) = 2^7 \bmod 33$
   $c(m) = 128 \bmod 33$
   $c(m) = 29$.

9. For cipher text *c*, the decryption function is
   $m(c) = c^d \bmod \varphi(n)$
   $m(c) = 29^3 \bmod 33$
   $m(c) = 24389 \bmod 33$
   $m(c) = 2$.

Advantages of RSA

- Very fast and simple encryption.
- Easier to implement.
- Easier to understand.
- Widely deployed, better industry support.

Disadvantages of RSA

- Very slow key generation.
- Slow signing and decryption, which are slightly tricky to implement securely.
- Key is vulnerable to various attacks if poorly implemented.

Introduction to Diffie-Hellman Algorithm

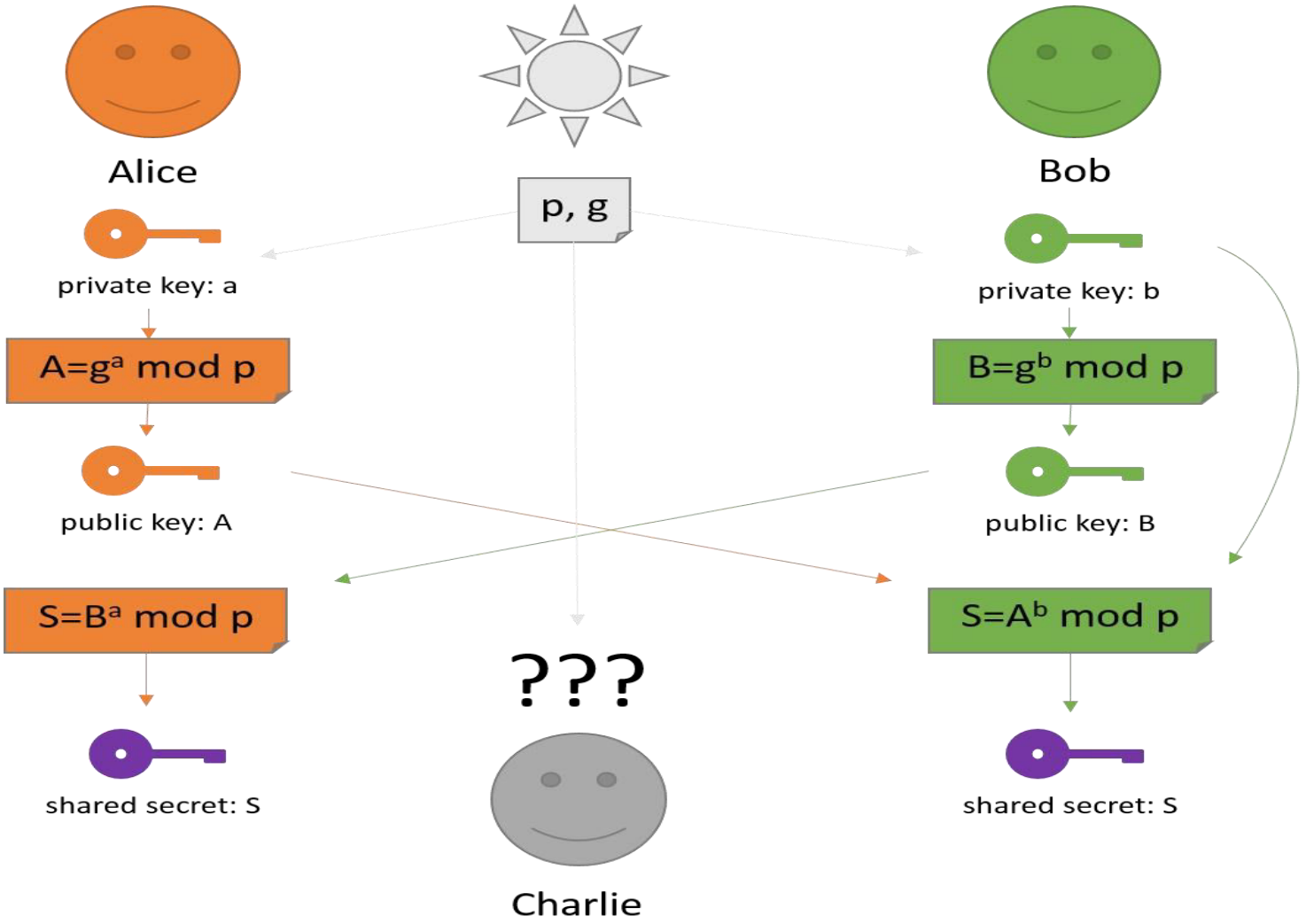
- **Diffie–Hellman key exchange** (**D–H**) is a specific method of securely exchanging cryptographic keys over a public channel.

- Traditionally, secure encrypted communication between two parties requires that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier.

- The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel.

- At the end of the communication both sender and receiver have the same key.

Working of Diffie-Hellman



Diffie-Hellman Algorithm

1. Alice and Bob agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).

2. Alice chooses a secret integer $\mathbf{a = 6}$, then sends Bob

   $A = g^{a} \bmod p$

   $A = 5^{6} \bmod 23$

   $A = 8$

3. Bob chooses a secret integer $\mathbf{b = 15}$, then sends Alice

   $B = g^{b} \bmod p$

   $B = 5^{15} \bmod 23$

   $B = 19$

4. Alice computes $s = B^a \bmod p$

   $s = 19^6 \bmod 23 = 2$

5. Bob computes $s = A^b \bmod p$

   $s = 8^{15} \bmod 23 = 2$

6. Alice and Bob now share a secret (the number **2**).

   Hence both Alice and Bob have arrived at the same value s.

Advantage of Diffie-Hellman Algorithm

- 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.

Disadvantages of Diffie-Hellman Algorithm

- Can not be used for asymmetric key exchange.
- Can not be used for signing digital signatures.
- The nature of the Diffie-Hellman key exchange does make it susceptible to man-in-the-middle attacks since it doesn't authenticate either party involved in the exchange.

Thank You