Information Assurance and Security

Chapter Two

Brief Overview of Commercial Issues

December 2022

What is Cryptography

- Is the mathematical “scrambling” of data so that only someone with the necessary key can “unscramble” it.
- It is the art of achieving security by encoding messages to make them non readable.
- Cryptography also allows senders and receivers to authenticate each other through the use of key pairs.
- There are various types of algorithms for encryption, some common algorithms include:

Cont'd

Secret Key Cryptography (SKC)

- Here only one key is used for both encryption and decryption.
- This type of encryption is also referred to as symmetric encryption.
- Example:
  - Data Encryption Standard (DES)-uses a 56-bit key
  - Advanced Encryption Standard (AES) - uses 128-bit, a 192-bit or a 256-bit key.

Cont'd

Public Key Cryptography (PKC)

- Here two keys are used.
- This type of encryption is also called asymmetric encryption.
- One key is the public key and anyone can have access to it.
- The other key is the private key, and only the owner can access it.
- The sender encrypts the information using the receiver's public key.
- The receiver decrypts the message using his/her private key.
- Example:
  - RSA, Diffie-Hellman, ECC

Cont'd

Hash Function

- These are different from SKC and PKC.
- They have no key at all and are also called one-way encryption.
- Hash functions are mainly used to ensure that a file has remained unchanged.

Encryption

- Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users.
- This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text.
- This encoded data may only be decrypted or made readable with a key.

Common Terms in Cryptography

Plain text

- This is the original message or data that is fed into the algorithm as input.

Encryption or Encipher

- the process of converting or codifying the original message into something cryptic form.

Encryption algorithm:

- The encryption algorithm performs various substitutions and transformations on the plaintext.

Secret key:

- The secret key is also input to the algorithm.
- The strength of the algorithm is depend on the key.

Cont'd

Cipher text:

- This is the scrambled message produced as output.
- It depends on the plaintext and the secret key.
- For a given message, two different keys will produce two different cipher texts.

Decryption or Decipher

- the process of converting the cryptic message into its corresponding form

Decryption algorithm:

- This is essentially the encryption algorithm run in reverse.
- It takes the cipher text and the same secret key and produces the original plaintext.

Cont'd

Cryptography:

- study of encryption principles/methods.

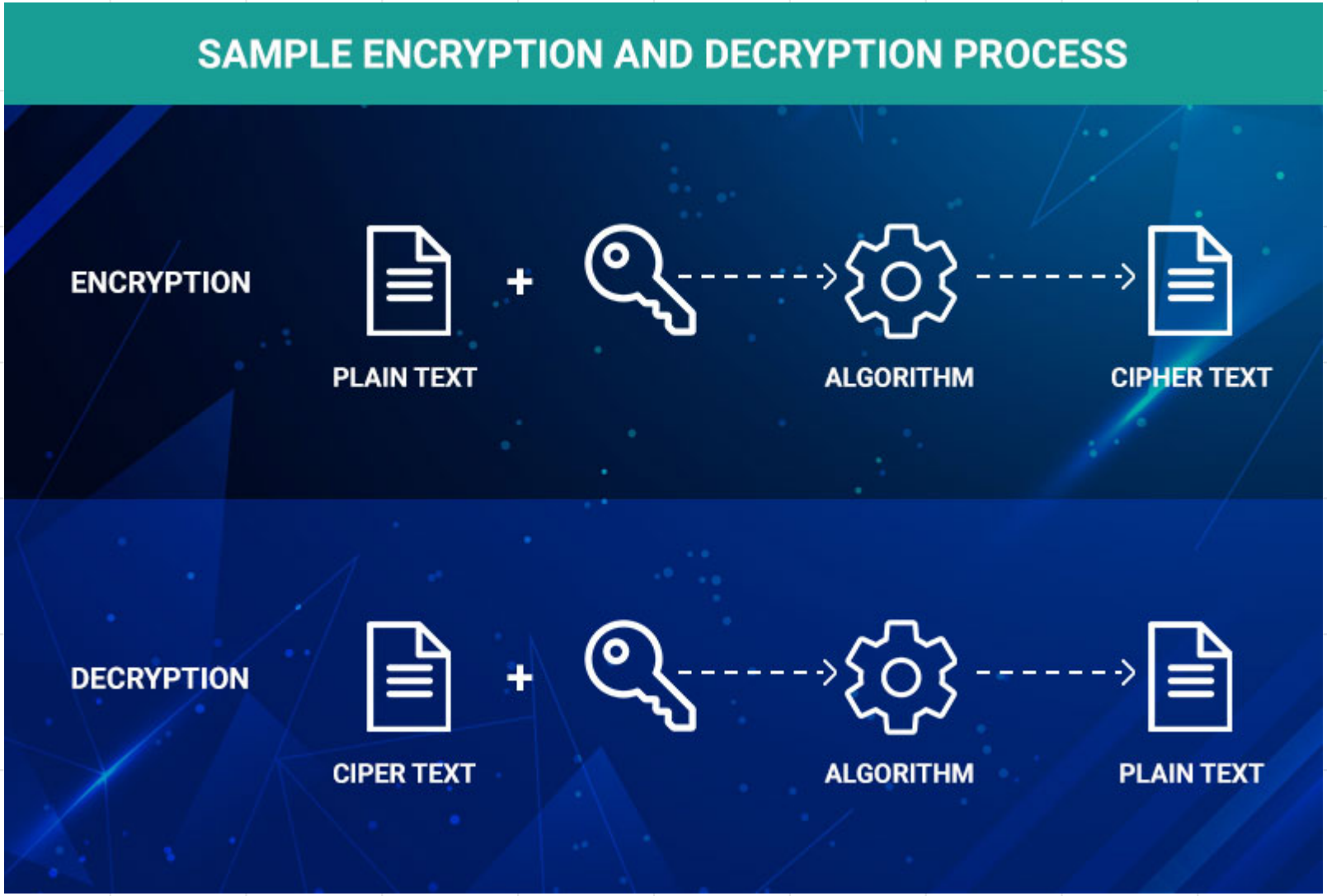
Cryptanalysis (codebreaking):

- the study of principles/ methods of deciphering cipher text without knowing key.

Cryptology:

- the field of both cryptography and cryptanalysis.

How Encryption and Decryption Algorithm work?

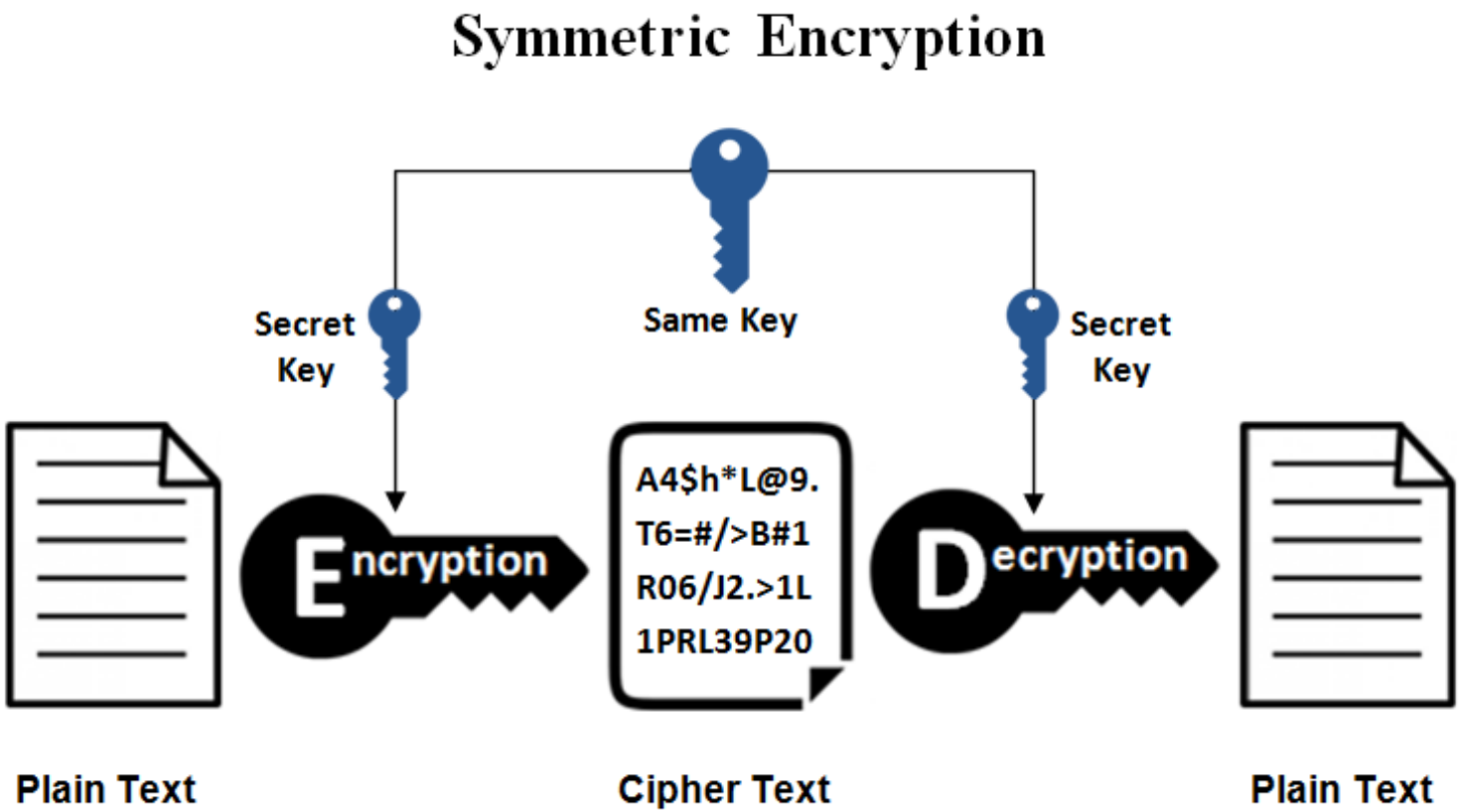


Cryptosystem

- Has five-tuple (P, C, K, and E, D), where the following are satisfied:
  1. P is a finite set of possible plaintexts.
  2. C is a finite set of possible ciphertexts.
  3. K the key space, is a finite set of possible keys
  4. E (encryption rule)
  5. D (decryption rule).

$$E_k(P) = C \ \ and \ \ D_k(C) = P$$

Symmetric/Secret/Private key Cryptography



Classical substitution Ciphers

- It encrypt the plaintext by swapping each letter or symbol in the plaintext by a different symbol as directed by the key.

Ceasar cipher

- It is the earliest and simplest methods of encryption technique.
- It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.
- The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,. . . , Z = 25.
- Encryption and decryption formula for Ceasar cipher.

$$En(x) = (x + n) \bmod 26$$

$$Dn(x) = (x - n) \bmod 26$$

Cryptanalysis of Caesar Cipher

- Only have 26 possible ciphers.
- The attacker attempts to use all possible permutations and combinations is called a brute-force attack.
- A brute force search could simply try each in turn.
- Break ciphertext "QHWZRUN VHFXULWB FODVV"

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

Cont'd

Mono-alphabetic cipher

- Rather than just shifting the alphabet this could shuffle (jumble) the letters arbitrarily.
- Now imagine that rather than using a uniform scheme for all the alphabets in a given plain text message, this uses random substitutions.
- This means that in a given plain text message, each A can be replaced by any other alphabet (B through Z), each B can also be replaced by any other random alphabet (A or C through Z) and so on.
- There is no relation between the replacement of B and replacement of A.

Cont'd

- Plain:A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- Cipher: D K V Q F I B J W P E S C X H T M Y A U O L R G Z N
- Example: for a given Plaintext: "if we wish to replace letters?
  The ciphertext would be: WI RF RWAJ UH YFTSDVF SFUUFYA
- In monolaphabetic cipher we have a total of $26! = 4x10^{26} keys$.
- With so many keys, might think is secure but would be WRONG.
- The problem is language characteristics.

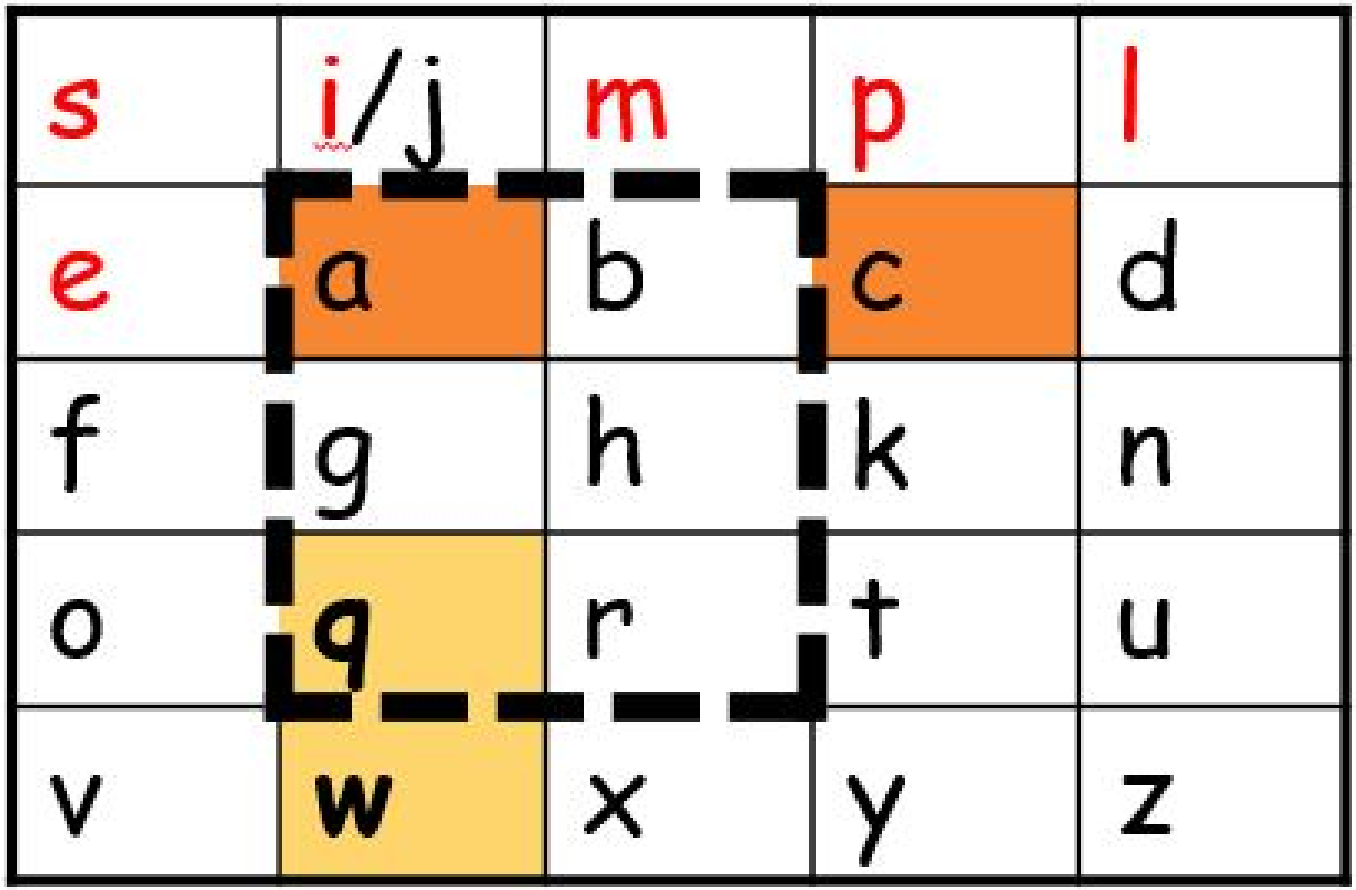
Cont'd

Play-fair Cipher

- Not even the large number of keys in a mono-alphabetic cipher provides security.
- One approach to improving security was to encrypt multiple letters.
- Plaintext is encrypted two letters at a time.
- A 5X5 matrix of letters based on a keyword.
- Fill in letters of keyword ((I and J aren't distinguished).
- fill rest of matrix with other letters.

Cont'd

- Example: Using the keyword simple



Cont'd

Encrypting and Decrypting of Playfair Cipher

- Use filler letter to separate repeated letters.
  - Eg. "balloon" encrypts as "ba lx lo on" Encrypt two letters together.
- Same row– >followed letters
  - If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right.
  - ac-bd
- Same column–> letters under
  - If both the letters are in the same column, take the letters below each one.
  - qw-wi
- Otherwise—>square's corner at same row
  - If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.
  - ar-bq

Cont'd

Activity

- Construct the playfair matrix using the keyword: MONARCHY ?
- Plaintext: Ethiopia

Security of Playfair Cipher

- security much improved over monoalphabetic
- But, still has much of plaintext structure.

Polyalphabetic Ciphers

- Another approach to improving security is to use multiple cipher alphabets called polyalphabetic substitution ciphers.
- Makes cryptanalysis harder with more alphabets to guess and flatter frequency distribution.
- Use a key to select which alphabet is used for each letter of the message.
- Use each alphabet in turn.
- Repeat from start after end of key is reached.

Cont'd

Vigenère Cipher

- Simplest polyalphabetic substitution cipher
- Effectively multiple caesar ciphers.
- key is multiple letters long K = k1 k2 ... kd
- i^{th} letter specifies i^{th} alphabet to use.

Example

- Write the plaintext out.
- Write the keyword repeated above it
- Use each key letter as a caesar cipher key.
- Encrypt the corresponding plaintext letter using keyword deceptive
- key: d e c e p t i v e d e c e p t i v e d e c e p t i v e
- plaintext: w e a r e d i s c o v e r e d s a v e y o u r s e l f
- ciphertext:Z I C VT WQNGRZGVT WAV ZHCQ YGLMGJ

Cont'd

Security of Vigenère Ciphers

- Have multiple ciphertext letters for each plaintext letter.
- Hence letter frequencies are obscured but not totally lost.

Web Services Security (WS-Security / WSS)

- A Web service is a service offered by an electronic device to another electronic device, communicating with each other via the World Wide Web (WWW).
- A web service enables communication among various applications by using open standards such as HTML, XML, WSDL, and SOAP.
- SOAP (Simple Object Access Protocol)
  - It is an XML-based protocol for accessing web services.
  - It is platform independent and language independent protocol.
  - provides data transport for Web services.
- WSDL (Web Services Description Language)
  - Is an XML-based language for describing Web services.
- XML (eXtensible Markup Language)
  - Is used to encode all communications to a web service.

Cont'd

Web Services Security (WS Security)

- Is a specification that defines how security measures are implemented in web services to protect them from external attacks.
- It is a set of protocols that ensure security for SOAP-based messages by implementing the principles of confidentiality, integrity and authentication.
- The aim of WS-Security is to ensure that communication between two parties is not interrupted or interpreted by an unauthorized third party.
- The receiver needs to be assured that the message was indeed sent by the sender, and the sender should be assured the receiver cannot deny receiving the message.
- Finally, the data sent during communication should not be altered by an unauthorized source.

Web Services Security Standards

WS-Policy

- A standards-based framework for defining a Web service's security constraints and requirements.

WS-Security

- Is an extension to SOAP to apply security to Web services.

WS-trust

- Refers to a protocol defined for particularly controlling the issuance, renewal and validation of Web security tokens.

WS-secure conversation

- WS-secure conversation builds on top of WS -policy, WS - security and WS -trust to enable secure communication b/n client and service.

Cont'd

WS-Reliable Messaging

- Allows web services and clients to trust that when a message is sent, it will be delivered to the intended party.

Web Service Atomic Transaction

- Allows transaction based web services in which transactions can be rolled in the event of failure.

New Symmetric Key Cryptographic Algorithm

- This asymmetric cryptographic algorithm uses 2 keys (public key Private Key), in which these keys can be calculated ASCHI value of a letter (character).
- Note: as this algorithm is under research, you may found limitations/draw backs.

Cont'd

New Symmetric key Encryption algorithm

1. Generate the ASCII value of the letter.
2. Generate the corresponding binary value of it.
   [Binary value should be 8 digits e.g. for decimal 32 binary number should be 00100000]
3. Reverse the 8 digit's binary number
4. Take a 4 digits divisor (>=1000) as the Key
5. Divide the reversed number with the divisor
6. Store the remainder in first 3 digits and quotient in next 5 digits (remainder and quotient wouldn't be more than 3 digits and 5 digits long respectively. If any of these are less then 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the cipertext i.e. encrypted text. Now store the remainder in first 3 digits quotient in next 5 digits.

Cont'd

New Symmetric key Decryption algorithm

1. Multiply last 5 digits of the ciphertext by the Key.
2. Add first 3 digits of the ciphertext with the result produced in the previous step.
3. If the result produced in the previous step i.e. step 2 is not an 8-bit number we need to make it an 8- bit number
4. Step 4: Reverse the number to get the original text i.e. the plaintext.

Asymmetric/Public key Cryptography

- Asymmetric type of cryptography is a secret writing of messages or information in between sender and receiver with two different keys used in between two parties for encryption and decryption processes.
- Asymmetric key cryptography uses two separate keys: one private and one public.
- This uses one key for encryption and another for decryption.
- Public Key Cryptography provides protection against internet based attacks through:
  - Encryption and Decryption allows two communicating parties to disguise information they send to each other.
  - Tamper detection allows the recipient of information to verify that it has not been modified in transit.
  - Authentication allows the recipient of information to determine its origin by confirming the sender identity.
  - Non repudiation prevents the sender of information from claiming at a later date that the information was never sent.

Cont'd

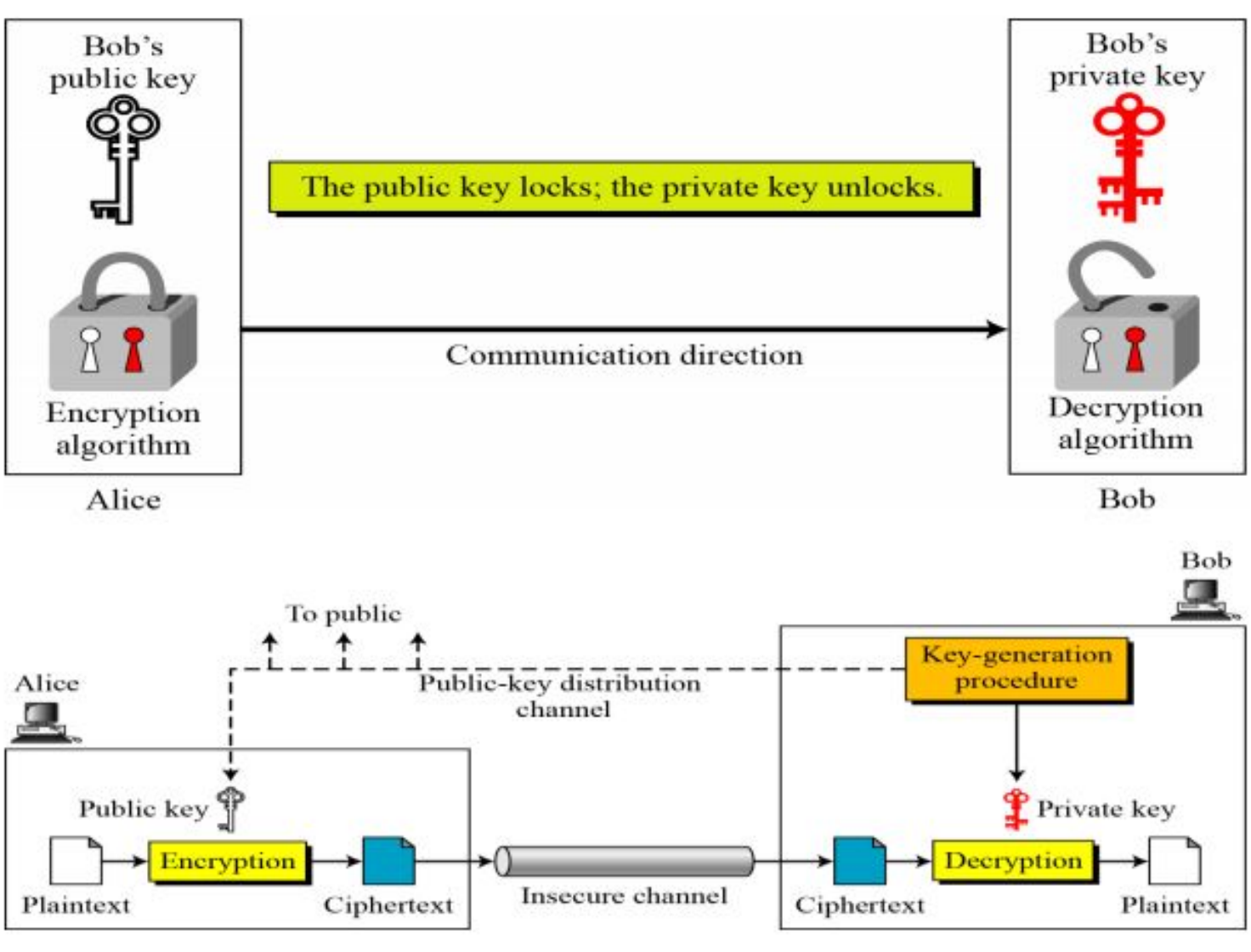


Figure: Asymmetric key cryptography

Difference between SKC and AKC

Symmetric Key Cryptography

- The same algorithm with the same key is used for encryption and decryption.
- The key must be kept secret.
- The encryption process is very fast.
- The length of key used is 128 or 256 bits

Asymmetric Key Cryptography

- One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
- One of the two keys must be kept secret.
- The encryption process is slow.
- The length of key used is 2048 or higher.


Thank You!