SLIIT

Discover Your Future

IE2022 – Introduction to Cyber Security

Lecture - 07

Cryptography III - Symmetric-Key Algorithms

Mr. Amila Senarathne

SLIIT
FACULTY OF COMPUTING

Cryptographic Hash Functions and Symmetric-Key Algorithms

- Reading Assignment
  - CCNA Security Curriculum, Chapter 7: Cryptographic Systems

- Supplementary text
  - W. Stallings and L. Brown, “Computer Security, Principles and Practice, 2nd edition, Pearson, 2012, Chapter 2 :Cryptographic Tools.

Topics to be discussed

- Symmetric Encryption Algorithms
- Symmetric Encryption Techniques
  - Block Ciphers
  - Stream Ciphers
- Choosing an Encryption Algorithm

Cryptology - The Secret Is in the Keys

- Authentication, integrity, and data confidentiality are implemented in many ways using various protocols and algorithms. Choice depends on the security level required in the security policy.

	Integrity	**Authentication**	**Confidentiality**
Common cryptographic hashes, protocols, and algorithms	MD5 (weaker) SHA (stronger)	HMAC-MD5 HMAC-SHA-1 RSA and DSA	DES (weaker) 3DES AES (stronger)

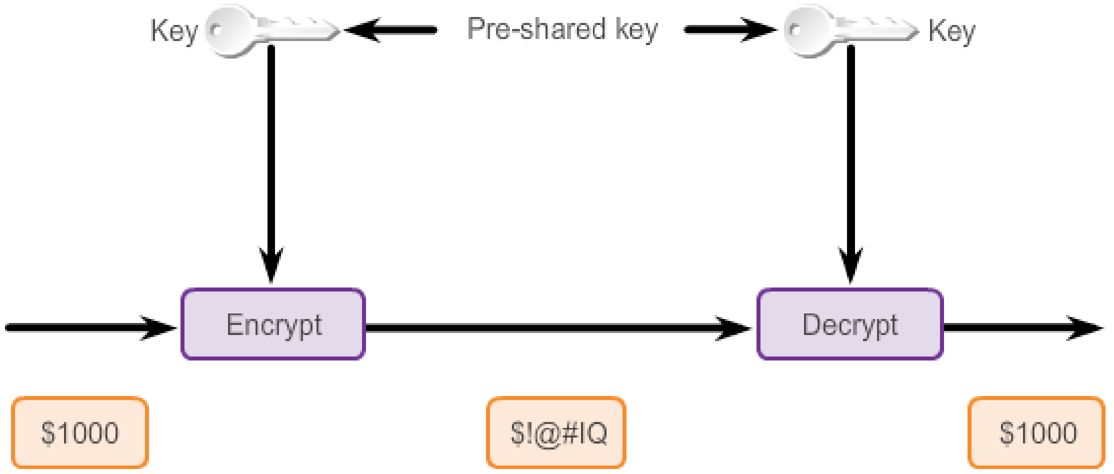
CONFIDENTIALITY

Cryptographic Encryption

- Cryptographic encryption can provide confidentiality at several layers of the OSI model by incorporating various tools and protocols:
  - Proprietary link-encrypting devices provide data link layer confidentiality.
  - Network layer protocols, such as the IPsec protocol suite, provide network layer confidentiality.
  - Protocols, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), provide session layer confidentiality.
  - Secure email, secure database session (Oracle SQL*net), and secure messaging (Lotus Notes sessions) provide application layer confidentiality.

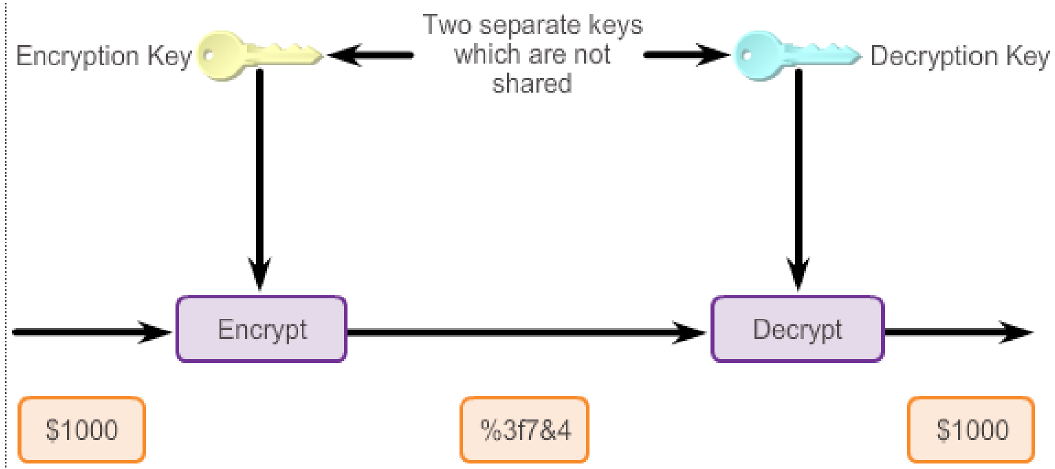
Symmetric Encryption Algorithms

- Symmetric encryption algorithms characteristics include:
  - Symmetric encryption algorithms are best known as shared-secret key algorithms.
  - The usual key length is 80 to 256 bits.
  - A sender and receiver must share a secret key.
  - They are usually quite fast (wire speed), because these algorithms are based on simple mathematical operations.
  - Examples of symmetric encryption algorithms are DES, 3DES, AES, IDEA, RC2/4/5/6, and Blowfish.



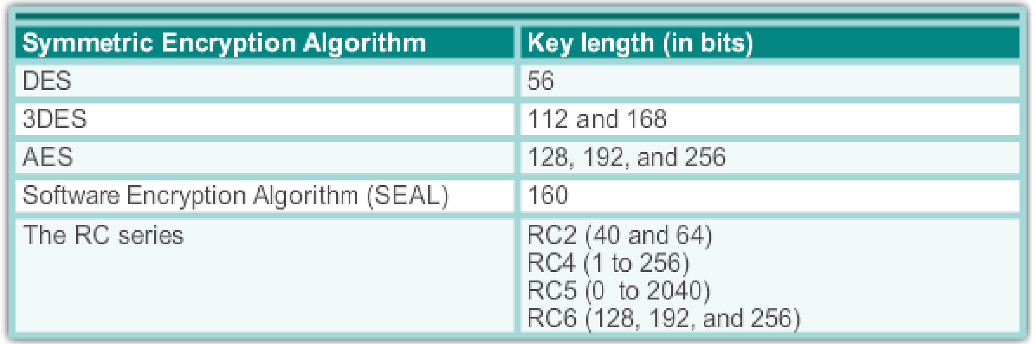
Asymmetric Encryption Algorithms

- Asymmetric encryption algorithms characteristics include:
  - Asymmetric encryption algorithms are best known as public key algorithms.
  - The usual key length is 512 to 4,096 bits.
  - A sender and receiver do not share a secret key.
  - These algorithms are relatively slow, because they are based on difficult computational algorithms.
  - Examples: RSA, ElGamal, elliptic curves, and DH.



Symmetric Encryption Algorithms

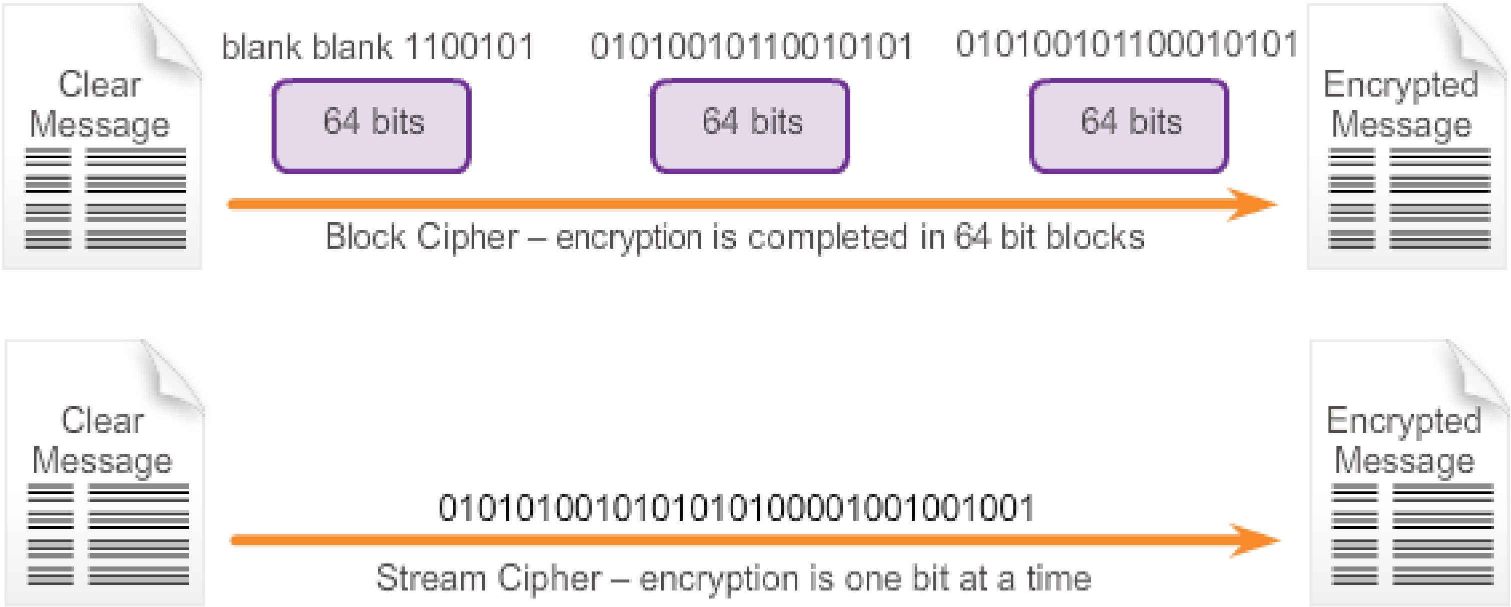
- Symmetric encryption algorithms, also called shared secret-key algorithms, use the same pre-shared secret key to encrypt and decrypt data. The pre-shared key is known by the sender and receiver before any encrypted communications begins.
- Because both parties are guarding a shared secret, the encryption algorithms used can have shorter key lengths. Shorter key lengths mean faster execution.
- For this reason symmetric algorithms are generally much less computationally intensive than asymmetric algorithms.



Symmetric Encryption Algorithm	Key length (in bits)
DES	56
3DES	112 and 168
AES	128, 192, and 256
Software Encryption Algorithm (SEAL)	160
The RC series	RC2 (40 and 64) RC4 (1 to 256) RC5 (0 to 2040) RC6 (128, 192, and 256)

Symmetric Encryption Techniques

- There are two types of encryption method used:
  - – Block Ciphers
  - – Stream Ciphers

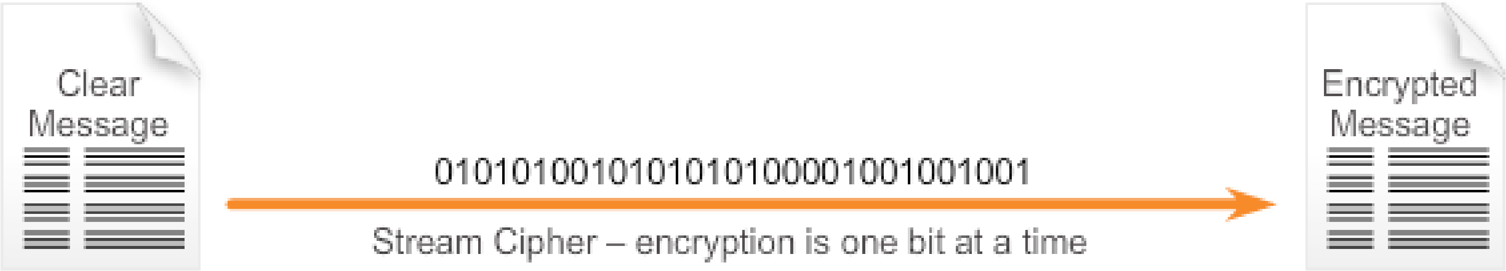


Block Ciphers

- Block ciphers transform a fixed-length block of plaintext into a common block of ciphertext of 64 or 128 bits.
  - Block size refers to how much data is encrypted at any one time.
  - The key length refers to the size of the encryption key that is used.
  - This ciphertext is decrypted by applying the reverse transformation to the ciphertext block, using the same secret key.
- Common block ciphers include:
  - DES with a 64-bit block size
  - AES with a 128-bit block size
  - RSA with a variable block size

Stream Ciphers

- Stream ciphers encrypt plaintext one byte or one bit at a time.
  - Think of it like a block cipher with a block size of one bit.
  - The Vigenère cipher is an example of a stream cipher.
  - Can be much faster than block ciphers, and generally do not increase the message size.
- Common stream ciphers include:
  - A5 used to encrypt GSM cell phone communications.
  - RC4 cipher.
  - DES can also be used in stream cipher mode.



Choosing an Encryption Algorithm

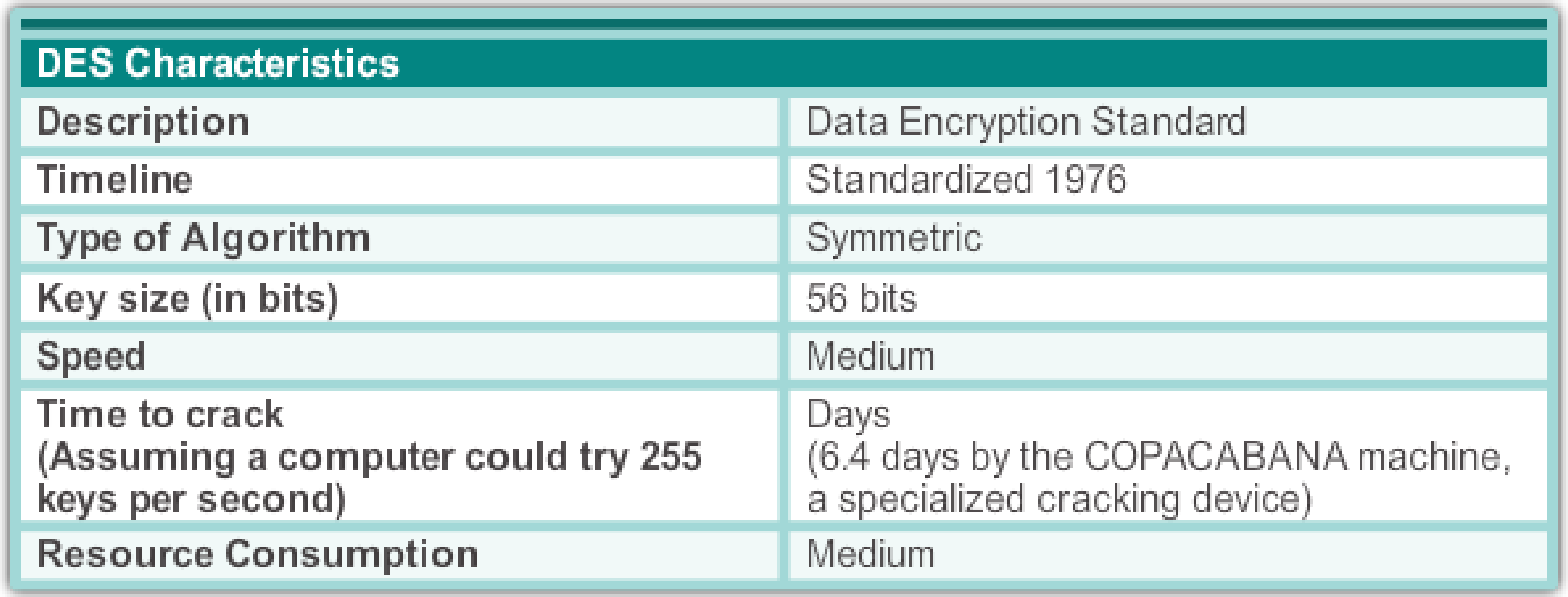
- Is the algorithm trusted by the cryptographic community? Algorithms that have been resisting attacks for a number of years are preferred.
- Does the algorithm adequately protects against brute-force attacks? With the appropriate key lengths, these attacks are usually considered unfeasible.
- Does the algorithm support variable and long key lengths?
- Does the algorithm have export or import restrictions?

Choosing an Encryption Algorithm

	DES	3DES	AES
Is the algorithm trusted by the cryptographic community?	Been replaced by 3DES	Yes	Verdict is still out
Does the algorithm adequately protect against brute-force attacks?	No	Yes	Yes

Data Encryption Standard

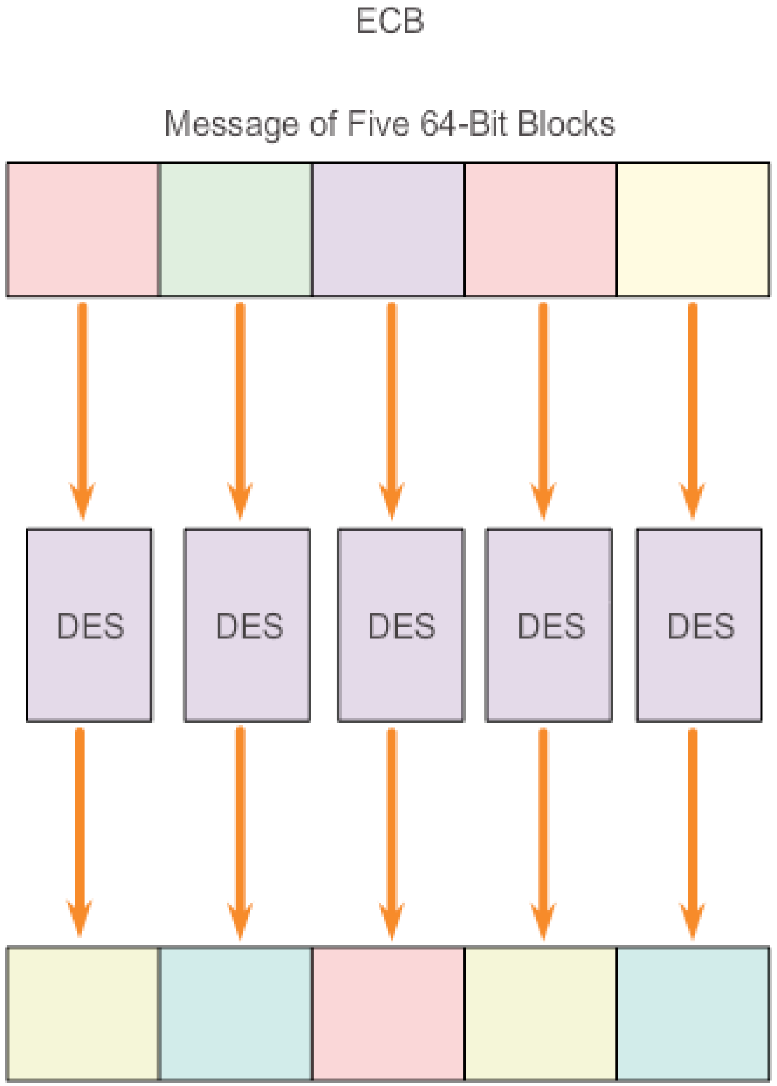
- The most popular symmetric encryption standard.
  - Developed by IBM
  - Thought to be unbreakable in the 1970s
  - Shared keys enable the encryption and decryption
- DES converts blocks of 64-bits of clear text into ciphertext by using an encryption algorithm.
  - The decryption algorithm on the remote end restores ciphertext to clear text.



DES Characteristics	
Description	Data Encryption Standard
Timeline	Standardized 1976
Type of Algorithm	Symmetric
Key size (in bits)	56 bits
Speed	Medium
Time to crack (Assuming a computer could try 255 keys per second)	Days (6.4 days by the COPACABANA machine, a specialized cracking device)
Resource Consumption	Medium

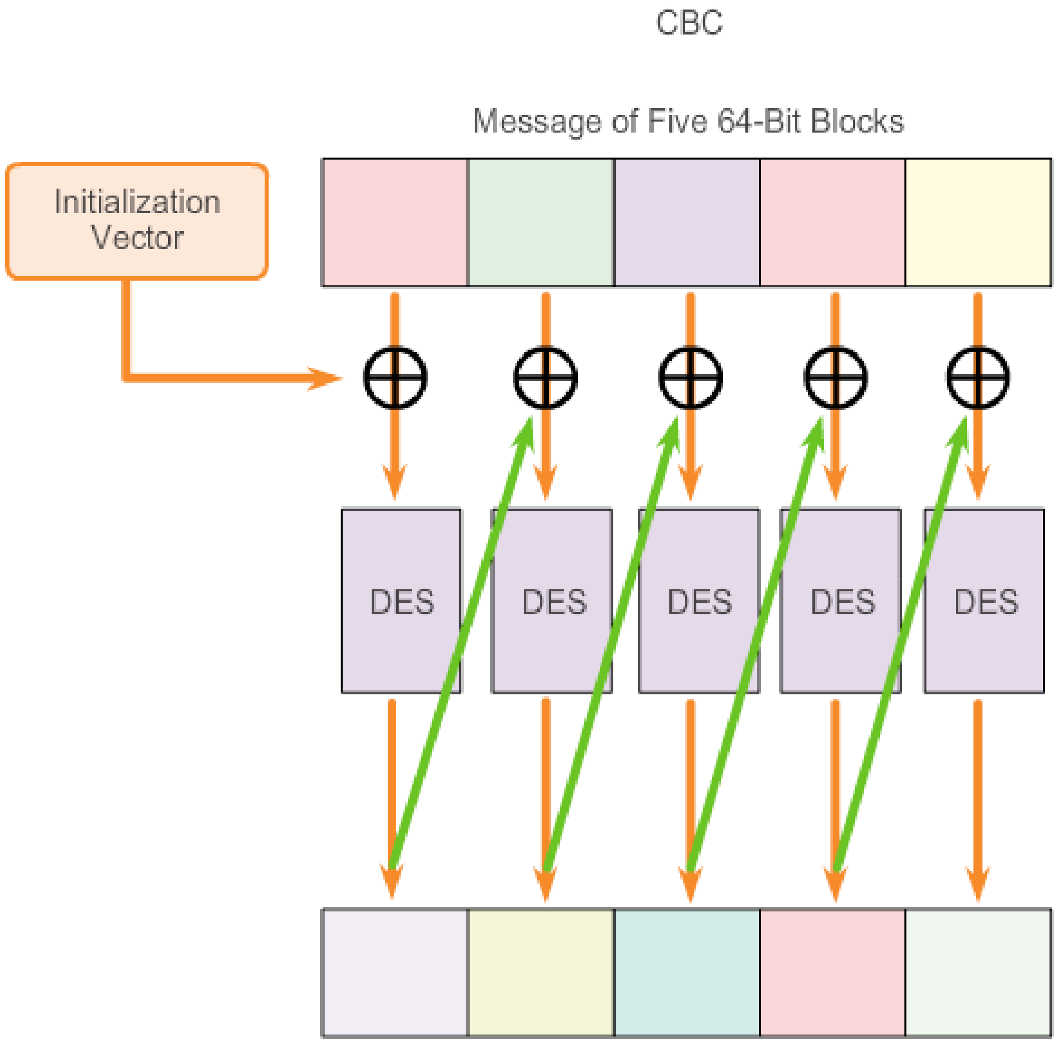
DES Operation - ECB

- ECB mode serially encrypts each 64-bit plaintext block using the same 56-bit key.
- If two identical plaintext blocks are encrypted using the same key, their ciphertext blocks are the same.
- Therefore, an attacker could identify similar or identical traffic flowing through a communications channel.



DES Operation - CBC

- CBC mode, each 64-bit plaintext block is XORed bitwise with the previous ciphertext block and then is encrypted using the DES key.
- The encryption of each block depends on previous blocks.
- Encryption of the same 64-bit plaintext block can result in different ciphertext blocks.



DES Operations Cont.

- To encrypt or decrypt more than 64 bits of data, DES uses two common stream cipher modes:
  - Cipher feedback (CFB), which is similar to CBC and can encrypt any number of bits, including single bits or single characters.
  - Output feedback (OFB) generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext.
- The cipher uses previous ciphertext and the secret key to generate a pseudo-random stream of bits, which only the secret key can generate.

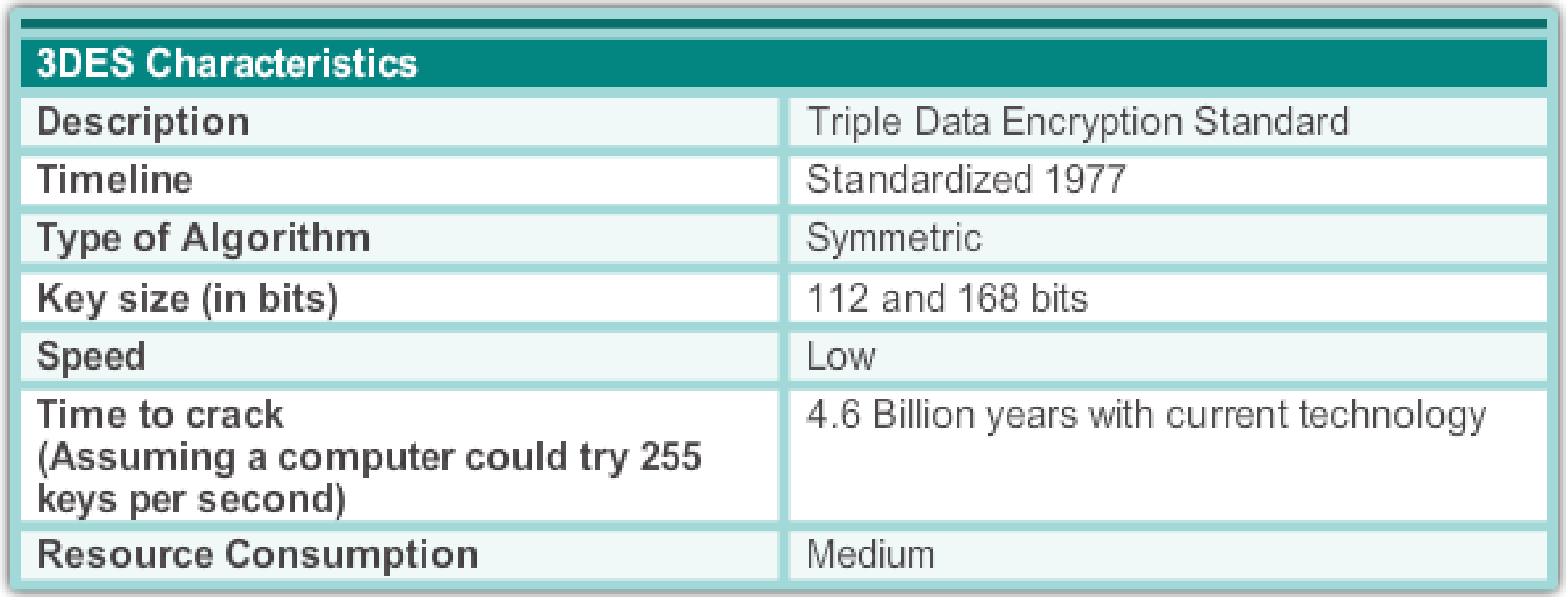
DES Summary

- Because of its short key length, DES is considered a good protocol to protect data for a very short time.
  - 3DES is a better choice to protect data, because it has an algorithm that is very trusted and has higher security strength.
- Recommendations:
  - Change keys frequently to help prevent brute-force attacks.
  - Use a secure channel to communicate the DES key from the sender to the receiver.
  - Consider using DES in CBC mode.
  - Test a key to see if it is a weak key before using it.

3DES - Improving DES with 3DES

- 3DES is 256 times stronger than DES.
- It takes a 64-bit block of data and performs three DES operations in sequence:
  - Encrypts, decrypts, and encrypts.
  - Requires additional processing time.
  - Can use 1, 2, or 3 different keys (when used with only one key, it is the same as DES).
- 3DES software is subject to U.S. export laws.

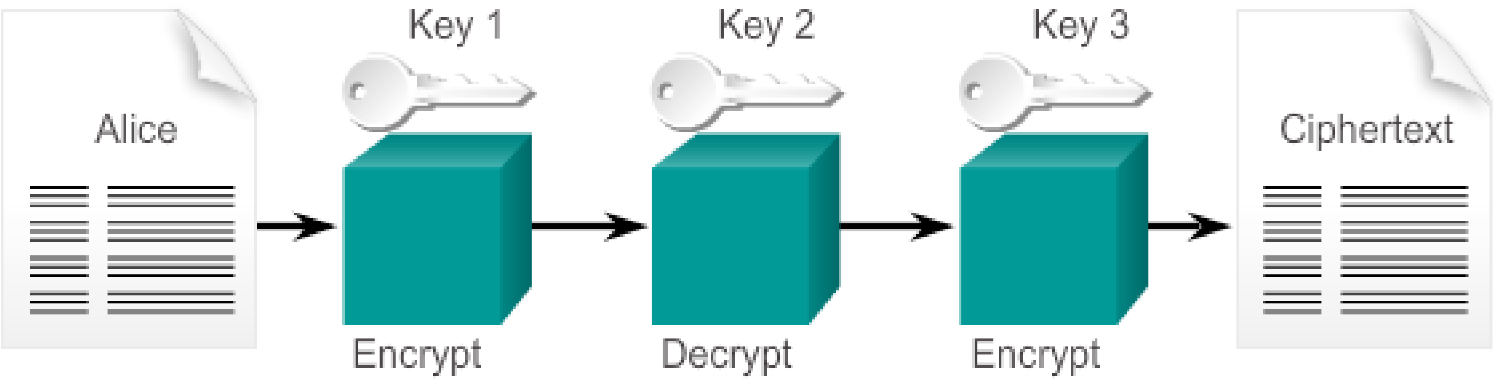
3DES - Improving DES with 3DES



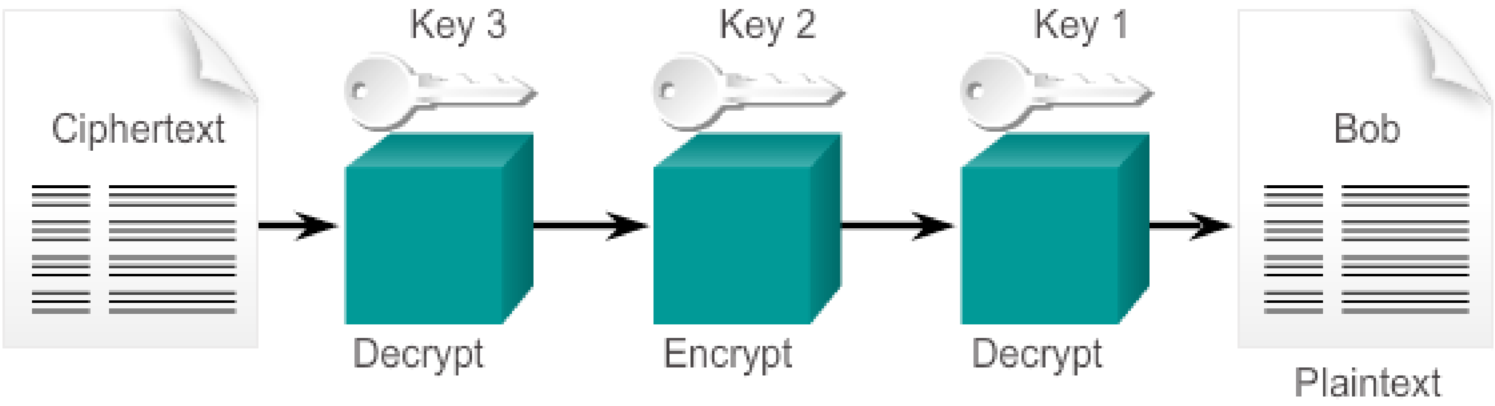
3DES Characteristics	
Description	Triple Data Encryption Standard
Timeline	Standardized 1977
Type of Algorithm	Symmetric
Key size (in bits)	112 and 168 bits
Speed	Low
Time to crack (Assuming a computer could try 255 keys per second)	4.6 Billion years with current technology
Resource Consumption	Medium

3DES - 3DES Operation

3DES Encryption



3DES Decryption



Advanced Encryption Standard (AES)

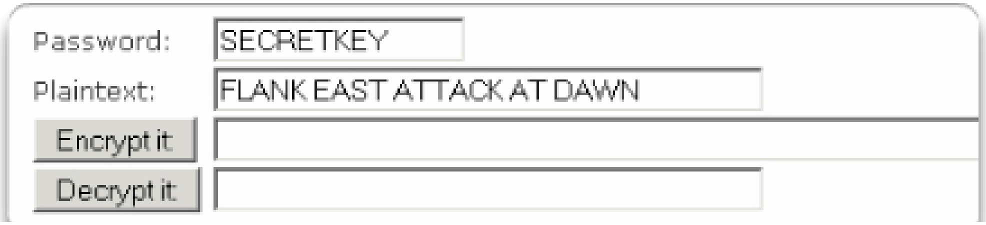
AES Origins

- 1997, the AES initiative was announced, and the public was invited to propose encryption schemes to replace DES.
- After a five-year standardization process in which 15 competing designs were presented and evaluated, the U.S. National Institute of Standards and Technology (NIST) selected the Rijndael block cipher as the AES algorithm..
  - Based on the Rijndael (“Rhine dahl”) algorithm.
  - It uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits.
  - All 9 combinations of key length and block length are possible.
- AES is now available in the latest Cisco router images that have IPsec DES/3DES functionality.

AES Summary

- AES was selected to replace DES for a number of reasons:
  - The key length of AES makes the key much stronger than DES.
  - AES runs faster than 3DES on comparable hardware.
  - AES is more efficient than DES and 3DES on comparable hardware, usually by a factor of five when it is compared with DES.
  - AES is more suitable for high-throughput, low-latency environments, especially if pure software encryption is used.
- However, AES is a relatively young algorithm and the golden rule of cryptography states that a mature algorithm is always more trusted.
- 3DES is, therefore, a more trusted choice in terms of strength, because it has been tested and analyzed for 35 years.

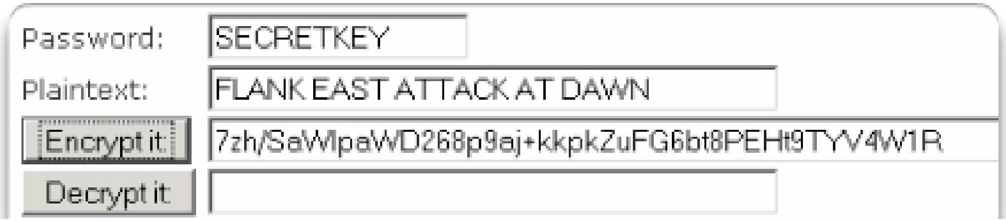
Advanced Encryption Standard



Password: SECRETKEY

Plaintext: FLANK EAST ATTACK AT DAWN

In this example, the SECRETKEY key and plaintext are entered.

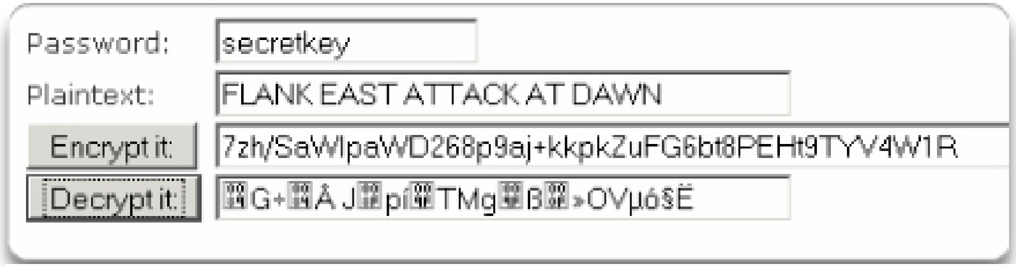


Password: SECRETKEY

Plaintext: FLANK EAST ATTACK AT DAWN

Encrypt it: 7zh/SaWlpaWD268p9aj+kkpkZuFG6bt8PEHt9TYV4W1R

They are now encrypted using 128 AES.



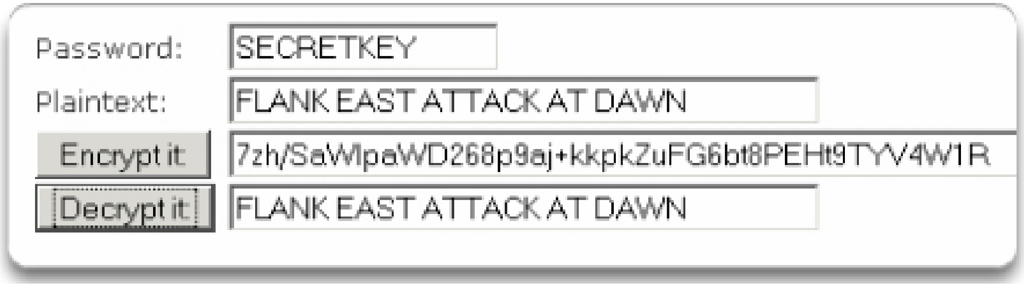
Password: secretkey

Plaintext: FLANK EAST ATTACK AT DAWN

Encrypt it: 7zh/SaWlpaWD268p9aj+kkpkZuFG6bt8PEHt9TYV4W1R

Decrypt it: ▯G+▯Å J▯pi▯TMg▯B▯»OVµó§Ë

An attempt at deciphering the text using a lowercase, and incorrect key.



Password: SECRETKEY

Plaintext: FLANK EAST ATTACK AT DAWN

Encrypt it: 7zh/SaWlpaWD268p9aj+kkpkZuFG6bt8PEHt9TYV4W1R

Decrypt it: FLANK EAST ATTACK AT DAWN

A second attempt at deciphering the text using the correct key displays the original plaintext.

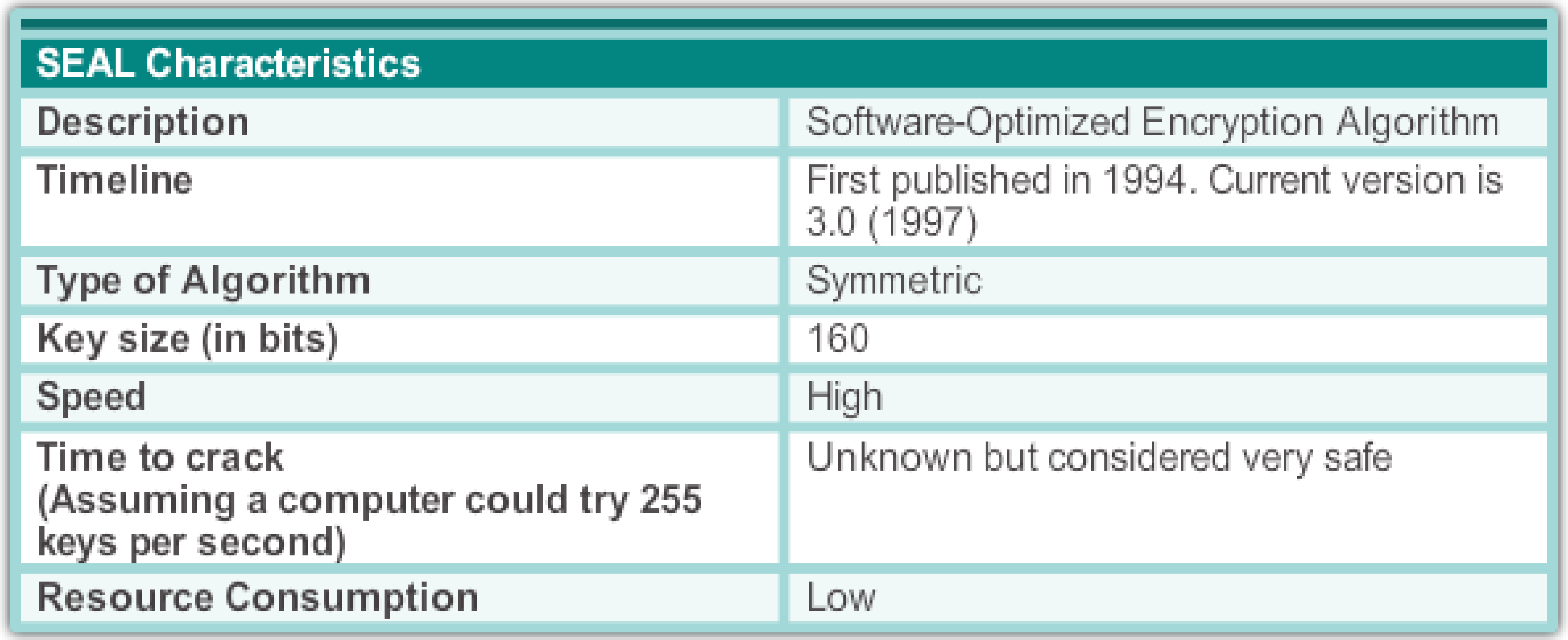
Software-Optimized Encryption Algorithm

- The Software-Optimized Encryption Algorithm (SEAL) is an alternative algorithm to software-based DES, 3DES, and AES.
  - Designed in 1993, it is a stream cipher that uses a 160-bit encryption key.
  - Because it is a stream cipher, data is continuously encrypted and, therefore, much faster than block ciphers.
  - However, it has a longer initialization phase during which a large set of tables is created using SHA (Secure Hash Algorithm).

- SEAL has a lower impact on the CPU compared to other software-based algorithms.

Software-Optimized Encryption Algorithm

SEAL Scorecard



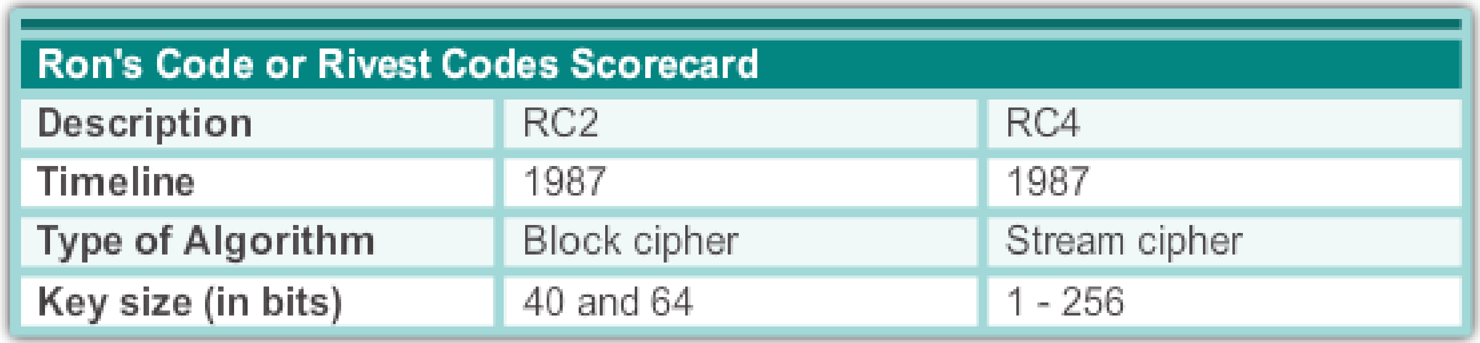
SEAL Characteristics	
Description	Software-Optimized Encryption Algorithm
Timeline	First published in 1994. Current version is 3.0 (1997)
Type of Algorithm	Symmetric
Key size (in bits)	160
Speed	High
Time to crack (Assuming a computer could try 255 keys per second)	Unknown but considered very safe
Resource Consumption	Low

RC Algorithms

- The RC algorithms were designed all or in part by Ronald Rivest, who also invented MD5.
- The RC algorithms are widely deployed in many networking applications because of their favorable speed and variable key-length capabilities.
- There are several variations of RC algorithms including:
  - RC2
  - RC4
  - RC5
  - RC6

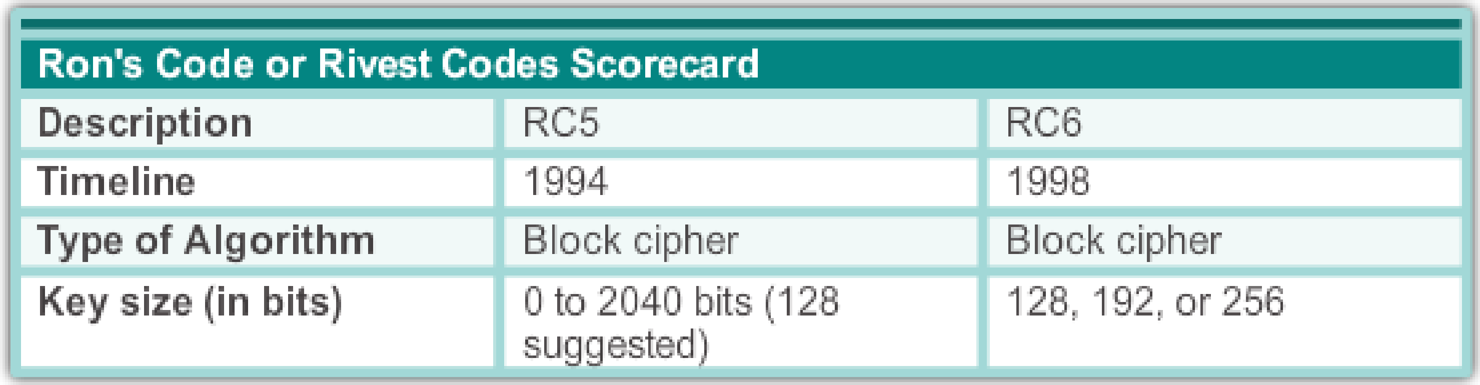
RC Algorithms Cont.

RC Algorithms Scorecard



Ron's Code or Rivest Codes Scorecard

Description	RC2	RC4
Timeline	1987	1987
Type of Algorithm	Block cipher	Stream cipher
Key size (in bits)	40 and 64	1 - 256



Ron's Code or Rivest Codes Scorecard

Description	RC5	RC6
Timeline	1994	1998
Type of Algorithm	Block cipher	Block cipher
Key size (in bits)	0 to 2040 bits (128 suggested)	128, 192, or 256

Questions?

End of Lecture 6