

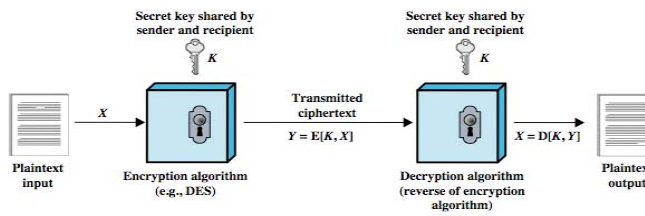
Lecture Outline

- Confidentiality with Symmetric Encry
 - Fundamental
 - Symmetric Block Encryption
- Hashing



© Madartists

Symmetric Encryption



- Plaintext:** This is the original message or data that is fed into the algorithm as input.
- Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- Secret key:** The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- If people know the algorithm, how is the ciphertext not deciphered by everyone?

Symmetric Encryption

- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

There are two requirements for secure use of symmetric encryption:

1. We need a strong encryption algorithm
2. Sender and receiver must securely obtain, & keep secure, the secret key

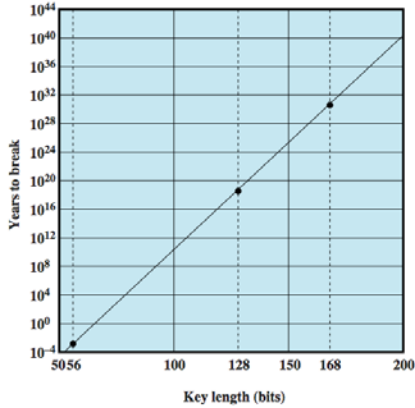
Attacking Symmetric Encryption

- There are 2 general approaches to attacking a symmetric encryption
- **cryptanalysis**
 - rely on nature of the algorithm
 - plus some knowledge of plaintext characteristics
 - even some sample plaintext-ciphertext pairs
 - exploits characteristics of algorithm to deduce specific plaintext or key
- **brute-force attack**
 - try all possible keys on some ciphertext until get an intelligible translation into plaintext

Exhaustive Key Search

Jul '98 Electronic Frontier Foundation (EFF) broke the DES encryption using a special-purpose "DES cracker" machine that was built for less than \$250,000 ([source code](#))

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



BUT: there is more to a key-search attack than simply running through all possible keys.

Unless known plaintext is provided, the analyst must be able to recognize plaintext as plaintext.

If the message is just plain text in English, then the result pops out easily.

If the message is some more general type of data, such as a numerical file, and this has been compressed, the problem becomes even more difficult to automate.

Adapted from Computer Security: Principles and Practice, Stallings and Lawrie

Symmetric Encryption Algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
 AES = Advanced Encryption Standard

- The most commonly used symmetric encryption algorithms are block ciphers
- A block cipher processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block
- The algorithm processes longer plaintext amounts as a series of fixed-size blocks. The most important symmetric algorithms, all of which are block ciphers, are the Data Encryption Standard (DES), triple DES, and the Advanced Encryption Standard (AES)

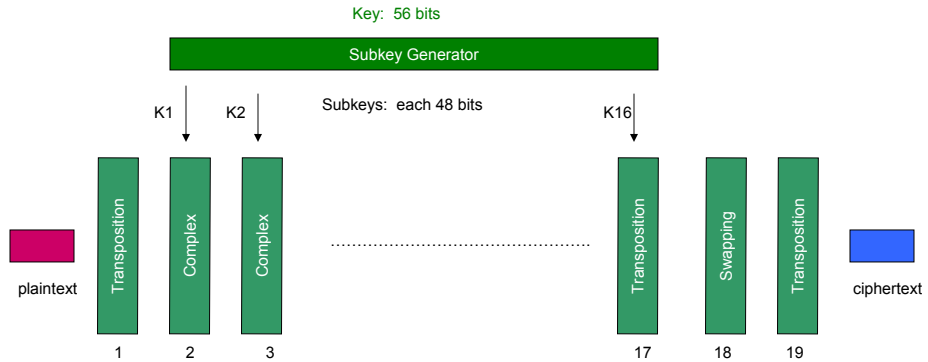
DES and Triple-DES

- Data Encryption Standard (DES) is the most widely used encryption scheme (1977)
 - adopted in 1977 by the National Bureau of Standards, now the NIST
 - uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block
 - concerns about algorithm & use of 56-bit key
- Triple-DES (1985)
 - repeats basic DES algorithm three times
 - using either two or three unique keys
 - much more secure but also much slower

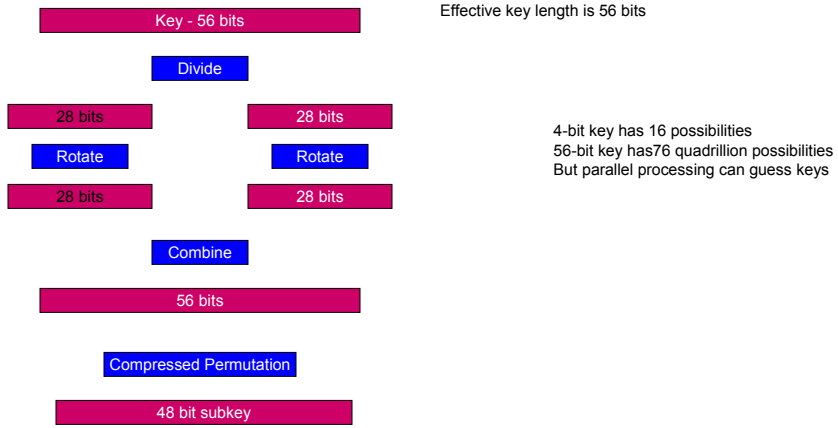
Data Encryption Standard (DES)

- National Security Agency (NSA) and National Institute of Standards and Technology (NIST) are responsible for the DES
 - NIST wanted a means of protecting sensitive but unclassified data. In the early '70s it invited vendors to submit data encryption algorithms
 - NIST accepted the already created Lucifer (IBM), but NSA modified it by reducing the key size from 128 bits to 64 bits and named it Data Encryption Algorithm (DEA) – not very original but...
- Was one of the most popular cryptographic algorithms
- Even though DES uses 64-bit encryption, only 56 bits are effectively used and 8 bits are used for parity
- DES is an example of bit-level encryption. Designed by IBM and adopted by the US government for nonmilitary and non classified use
- Encrypts a 64-bit plaintext, using a 56-bit key
- The text is put through 19 different and very complex procedures to create a 64-bit ciphertext
- The 56-bit key is no longer considered secure enough to be used – it has been broken in as little as 3.5 hours by fast computers

Data Encryption Standard (DES)



Data Encryption Standard (DES) – Subkey Generation





Advanced Encryption Standard (AES)

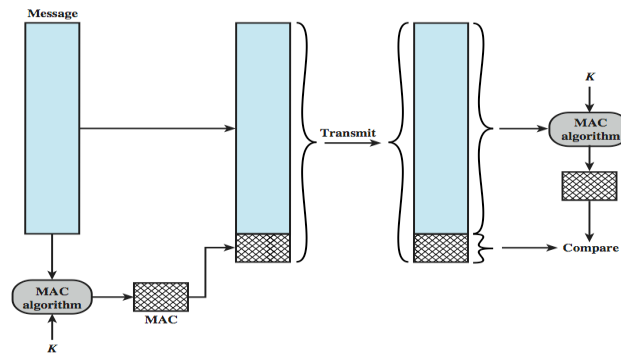
- Needed a better replacement for DES
- NIST called for proposals in 1997 for the new Advanced Encryption Standard (AES).
- The specifications were as follows:
 - have a security strength equal to or better than 3DES and significantly improved efficiency
 - symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits
 - Other evaluation criteria included security, computational efficiency, memory requirements, hardware and software suitability, and flexibility
- 5 finalists: Rijndael, MARS, RC6, Serpent, Twofish
- selected Rijndael in Nov 2001 - the Rijndael algorithm from Belgians, Vincent Rijmen and Joan Daemen -
- AES – elegant mathematical formula, very fast execution AES uses 128-bit (performs 9 rounds), 192-bit (performs 11 rounds), and 256 bit keys (performs 13 rounds), (1.1 * 10⁷⁷ possible keys)
- Estimate time to crack: 149 trillion years – benchmarked by a machine cracking DES in 1 second (Universe is only about 20 billion years old)
- now widely available commercially
- Other symmetric cryptography algorithms: IDEA (International Data Encryption Algorithm), Blowfish, RC5

Message Authentication

- Encryption protects against active attacks (falsification of data and transaction)
 - verifies received message is authentic
 - contents unaltered
 - from authentic source
 - timely (not delayed or replayed) and in correct sequence
 - can use conventional encryption
 - only sender & receiver have key needed
- or
- separate authentication mechanisms
 - append authentication tag to cleartext/ plaintext message

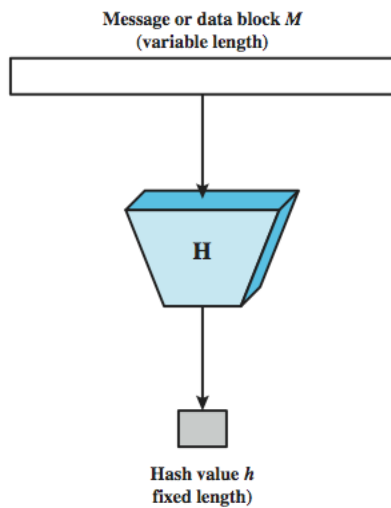
Message Authentication Codes

- One authentication technique involves the use of a secret key to generate a small block of data, known as a **message authentication code**, that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key K_{AB} . When A has a message to send to B, it calculates the message authentication code as a **function of the message and the key**: $MAC_M = F(K_{AB}, M)$. The message plus code are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new message authentication code.
- The receiver is assured that the message has not been altered.
 - The receiver is assured that the message is from the alleged sender.
 - If the message includes a sequence number, then the receiver can be assured of the proper sequence.



CSCI 415: Computer and Network Security Dr. Nazli Hardy Adapted from Computer Security: Principles and Practice, Stallings and Lawrie

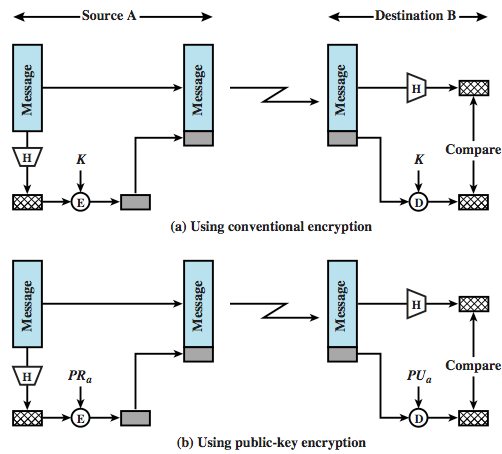
Secure Hash Functions



- An alternative to the message authentication code is the **one-way hash function**.
- As with the message authentication code, a hash function accepts a **variable-size message M** as input and produces a **fixed-size message digest H(M)** as output.
- Unlike the MAC, a hash function does not also take a secret key as input. To authenticate a message, the message digest is sent in addition to the message.
- The H(M) is intricately related to the actual message (length, characters, order)

CSCI 415: Computer and Network Security Dr. Nazli Hardy Adapted from Computer Security: Principles and Practice, Stallings and Lawrie

Message Authentication



Cryptography II – Symmetric and Hashing

Message Authentication

- Hashing is applied to any size data
- H produces a fixed-length output
- $H(x)$ is relatively easy to compute for any given x
- one-way property
 - computationally infeasible to find x such that $H(x) = h$
- weak collision resistance
 - computationally infeasible to find $y \neq x$ such that $H(y) = H(x)$
- strong collision resistance
 - computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$