1

SECURITY IN COMPUTING, FIFTH EDITION

Chapter 12: Details of Cryptography

1

2

Chapter 12 Objectives

- Learn basic terms and primitives of cryptography
- Deep dive into how symmetric encryption algorithms work
- Study the RSA asymmetric encryption algorithm
- Compare message digest algorithms
- Explain the math behind digital signatures
- Learn the concepts behind quantum cryptography

2

3

Methods of Cryptanalysis

- Break (decrypt) a single message
- Recognize patterns in encrypted messages
- Infer some meaning without even breaking the encryption, such as from the length or frequency of messages
- Easily deduce the key to break one message and perhaps subsequent ones
- Find weaknesses in the implementation or environment of use of encryption by the sender
- Find general weaknesses in an encryption algorithm

3

Cryptanalysis Inputs

- Ciphertext only
  - Look for patterns, similarities, and discontinuities among many messages that are encrypted alike
- Plaintext and ciphertext, so the cryptanalyst can see what transformations occurred
  - Known plaintext
  - Probable plaintext
  - Chosen plaintext

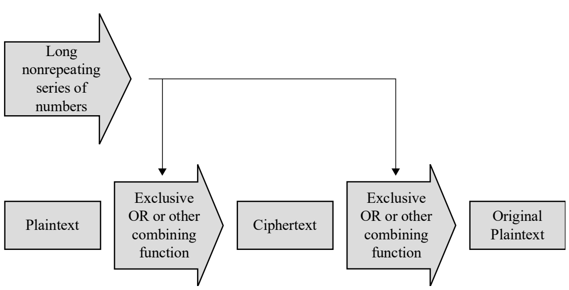
4

Cryptographic Primitives

- Substitution
  - One set of bits is exchanged for another
- Transposition
  - Rearranging the order of the ciphertext to break any repeating patterns in the underlying plaintext
- Confusion
  - An algorithm providing good confusion has a complex functional relationship between the plaintext/key pair and the ciphertext, so that changing one character in the plaintext causes unpredictable changes to the resulting ciphertext
- Diffusion
  - Distributes the information from single plaintext characters over the entire ciphertext output, so that even small changes to the plaintext result in broad changes to the ciphertext

5

One-Time Pads



6

Shannon's Characteristics of Good Ciphers

1. The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption
2. The set of keys and the enciphering algorithm should be free from complexity
3. The implementation of the process should be as simple as possible
4. Errors in ciphering should not propagate and cause corruption of further information in the message
5. The size of the enciphered text should be no larger than the text of the original message

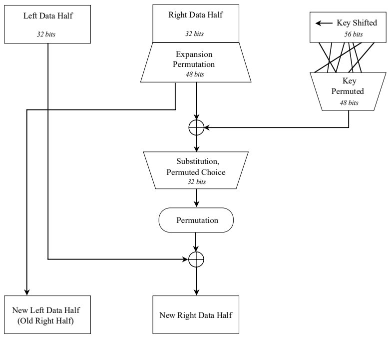
7

Properties of a Trustworthy Cryptosystem

- It is based on sound mathematics
- It has been analyzed by competent experts and found to be sound
- It has stood the test of time

8

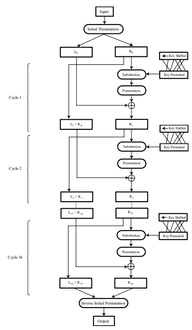
DES Algorithm



9

10

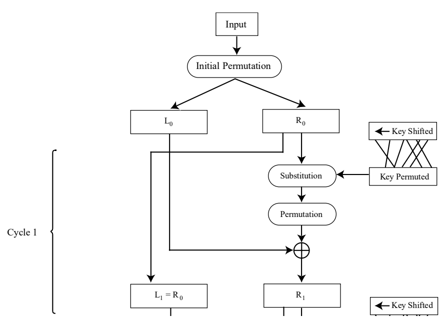
DES Algorithm (cont.)



10

11

DES Algorithm (cont.)

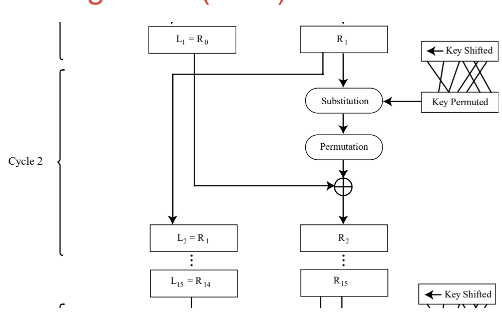


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

11

12

DES Algorithm (cont.)

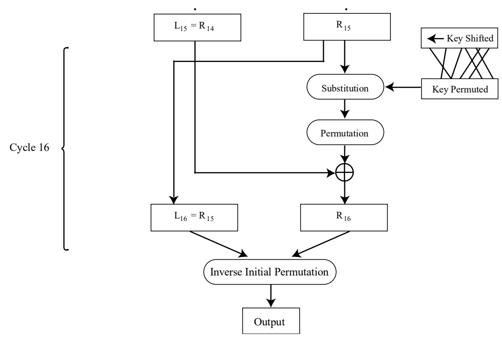


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

12

13

DES Algorithm (cont.)



13

14

DES Decryption

$$L_j = R_{j-1} \qquad (1)$$

$$R_j = L_{j-1} \oplus f(R_{j-1}, k_j) \qquad (2)$$

By rewriting these equations in terms of R_{j-1} and L_{j-1}, we get

$$R_{j-1} = L_j \qquad (3)$$

and

$$L_{j-1} = R_j \oplus f(R_{j-1}, k_j) \qquad (4)$$

Substituting (3) into (4) gives

$$L_{j-1} = R_j \oplus f(L_j, k_j) \qquad (5)$$

14

15

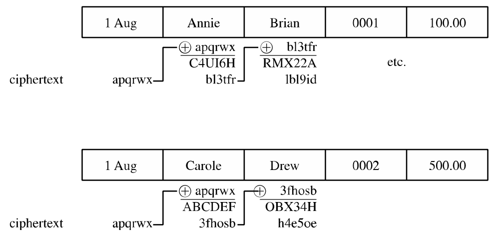
Chaining

- DES uses the same process for each 64-bit block, so two identical blocks encrypted with the same key will have identical output
- This provides too much information to an attacker, as messages that have common beginnings or endings, for example, are very common in real life, as is reuse of a single key over a series of transactions
- The solution to this problem is chaining, which makes the encryption of each block dependent on the content of the previous block as well as its own content

15

16

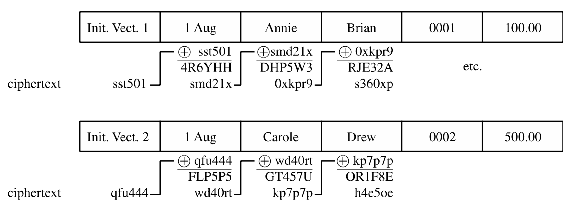
Simple Chaining Example



16

17

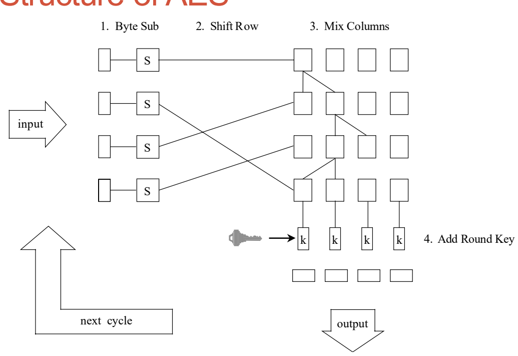
Initialization Vectors



17

18

Structure of AES



18

Longevity of AES

- Since its initial publication in 1997, AES has been extensively analyzed, and the only serious challenges to its security have been highly specialized and theoretical
- Because there is an evident underlying structure to AES, it will be possible to use the same general approach on a slightly different underlying problem to accommodate keys larger than 256 bits when necessary
- No attack to date has raised serious question as to the overall strength of AES

19

Asymmetric Encryption with RSA

- Since its introduction in 1978, RSA has been the subject of extensive cryptanalysis, and no serious flaws have yet been found
- The encryption algorithm is based on the underlying problem of factoring large prime numbers, a problem for which the fastest known algorithm is exponential in time
- Two keys, d and e, are used for decryption and encryption (they are interchangeable)
- The plaintext block P is encrypted as $P^e \bmod n$
- The decrypting key d is chosen so that $(P^e)^d \bmod n = P$

20

Detailed Description of RSA

The RSA algorithm uses two keys, d and e, which work in pairs, for decryption and encryption, respectively. A plaintext message P is encrypted to ciphertext C by

$$C = P^e \bmod n$$

The plaintext is recovered by

$$P = C^d \bmod n$$

Because of symmetry in modular arithmetic, encryption and decryption are mutual inverses and commutative. Therefore,

$$P = C^d \bmod n = (P^e)^d \bmod n = (P^d)^e \bmod n$$

This relationship means that one can apply the encrypting transformation and then the decrypting one, or the decrypting one followed by the encrypting one.

21

Deriving an RSA Key Pair

- The encryption key consists of the pair of integers (*e*, *n*), and the decryption key is (*d*, *n*)
- The value of *n* should be quite large, a product of two primes, *p* and *q*
- Typically, *p* and *q* are nearly 100 digits each, so *n* is approximately 200 decimal digits (about 512 bits) long
- A large value of *n* effectively inhibits factoring *n* to infer *p* and *q* (but time to encrypt increases as the value of *n* grows larger)
- A relatively large integer *e* is chosen so that *e* is relatively prime to $(p - 1) * (q - 1)$. An easy way to guarantee that *e* is relatively prime to $(p - 1) * (q - 1)$ is to choose *e* as a prime that is larger than both $(p - 1)$ and $(q - 1)$
- Finally, select *d* such that $e * d = 1 \bmod (p - 1) * (q - 1)$

22

Message Digests

- Previously introduced in Chapter 2, message digests are ways to detect changes to a block of data
- One-way hash functions are cryptographic functions with multiple uses:
  - They are used in conjunction with public-key algorithms for both encryption and digital signatures
  - They are used in integrity checking
  - They are used in authentication
  - They are used in communications protocols
- Modern hash functions meet two criteria:
  - They are one-way, meaning they convert input to a digest, but it is infeasible to start with a digest value and infer the input
  - They do not have obvious collisions, meaning that it is infeasible to find a pair of inputs that produce the same digest

23

Properties of Current Hash Standards

Algorithm	Maximum Message Size (bits)	Block Size (bits)	Rounds	Message Digest Size (bits)
MD5	2^{64}	512	64	128
SHA-1	2^{64}	512	80	160
SHA-2-224	2^{64}	512	64	224
SHA-2-256	2^{64}	512	64	256
SHA-2-384	2^{128}	1024	80	384
SHA-2-512	2^{128}	1024	80	512
SHA-3-256	unlimited	1088	24	256
SHA-3-512	unlimited	576	24	512

24

Digital Signatures

- As we initially saw in Chapter 2, digital signatures must meet two requirements and, ideally, satisfy two more:
  - *Unforgeable (mandatory):* No one other than the signer can produce the signature without the signer's private key
  - *Authentic (mandatory):* The receiver can determine that the signature really came from the signer
  - *Not alterable (desirable):* No signer, receiver, or any interceptor can modify the signature without the tampering being evident
  - *Not reusable (desirable):* Any attempt to reuse a previous signature will be detected by receiver
- The general way of computing digital signatures is with public key encryption:
  - The signer computes a signature value by using a private key
  - Others can use the public key to verify that the signature came from the corresponding private key

25

Elliptic Curve Cryptosystems

- While the RSA algorithm appears sufficiently strong, it has a different kind of flaw: It is patented
- An alternative form of asymmetric cryptography comes in the form of Elliptic Curve Cryptography (ECC)
- ECC has two advantages over RSA:
  - While some technologies using ECC are patented, the general algorithm is in the public domain
  - ECC can provide similar security to RSA using a shorter key length

26

Quantum Cryptography

- Based on physics, not mathematics, using light particles called photons
- It relies on our ability to measure certain properties of photons and on Heisenberg's uncertainty principle, which allows senders and receivers in quantum communication to easily detect eavesdroppers
- Implementations of quantum cryptography remain in the prototype stage, as creating practical photon guns and receivers is technically difficult
- While still not ready for widespread adoption, quantum cryptography may be practical within the next decade and would likely be a significant improvement over existing systems for encrypted communication

27

Summary

- Substitution, transposition, confusion, and diffusion are the basic primitives of cryptography
- DES is a relatively simple symmetric algorithm that, although no longer practical, is useful for studying technique
- Chaining and random initialization vectors are important techniques for preventing ciphertext repetition
- AES remains the modern standard for symmetric encryption almost 20 years after its introduction
- RSA is a popular and deceptively simple algorithm for asymmetric cryptography
- Message digests use one-way cryptographic hash functions to detect message modification
- Digital signatures use asymmetric encryption to detect forged messages
- While not yet ready for mainstream use, quantum cryptography will likely be a significant improvement over modern encrypted communication

28