SECURITY IN COMPUTING, FIFTH EDITION

Chapter 12: Details of Cryptography

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

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

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

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

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

Methods of Cryptanalysis

- Find weaknesses in the implementation or environment of use of encryption by the sender
- Find general weaknesses in an encryption algorithm

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

Methods of Cryptanalysis

- We start with a brief discussion of cryptanalysis
- How can we protect data from attackers?
  - Understand what attackers are trying to accomplish
  - How they are trying to accomplish it

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

Methods of Cryptanalysis

- Different methods are not mutually exclusive
- Which ones are applied will depend on:
  - Expertise of the attacker
  - What information is available to the attacker
  - What access is available to the attacker
  - Other constraints, such as time

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

Cryptanalysis Inputs

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

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

Cryptanalysis Inputs

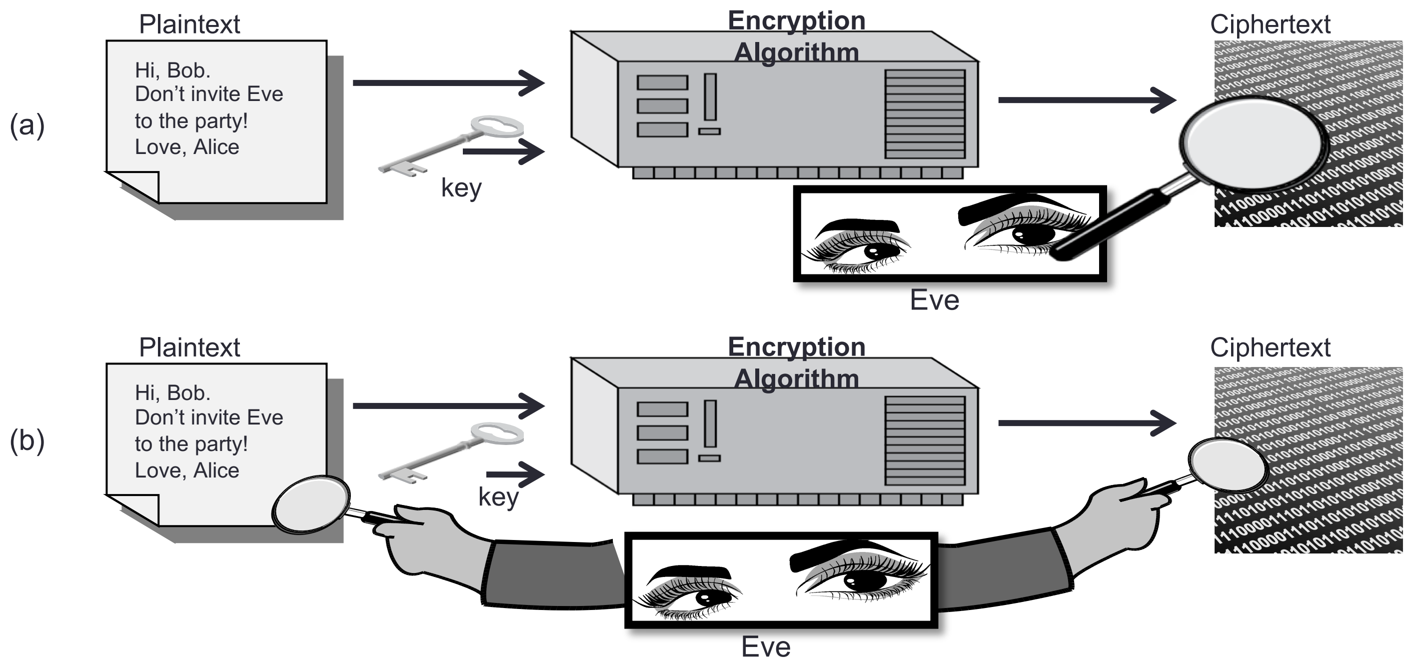
- Plaintext and ciphertext attacks:
  - Known plaintext:
    - the analyst has an exact copy of the plaintext and ciphertext
  - Probable plaintext:
    - message is very likely to have certain content, such as a date header
  - Chosen plaintext:
    - the attacker gains sufficient access to the system to generate ciphertext from arbitrary plaintext inputs

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

Attacks

- Attacker may have
  - collection of ciphertexts (***ciphertext only attack***)
  - collection of plaintext/ciphertext pairs (***known plaintext attack***)

Attacks

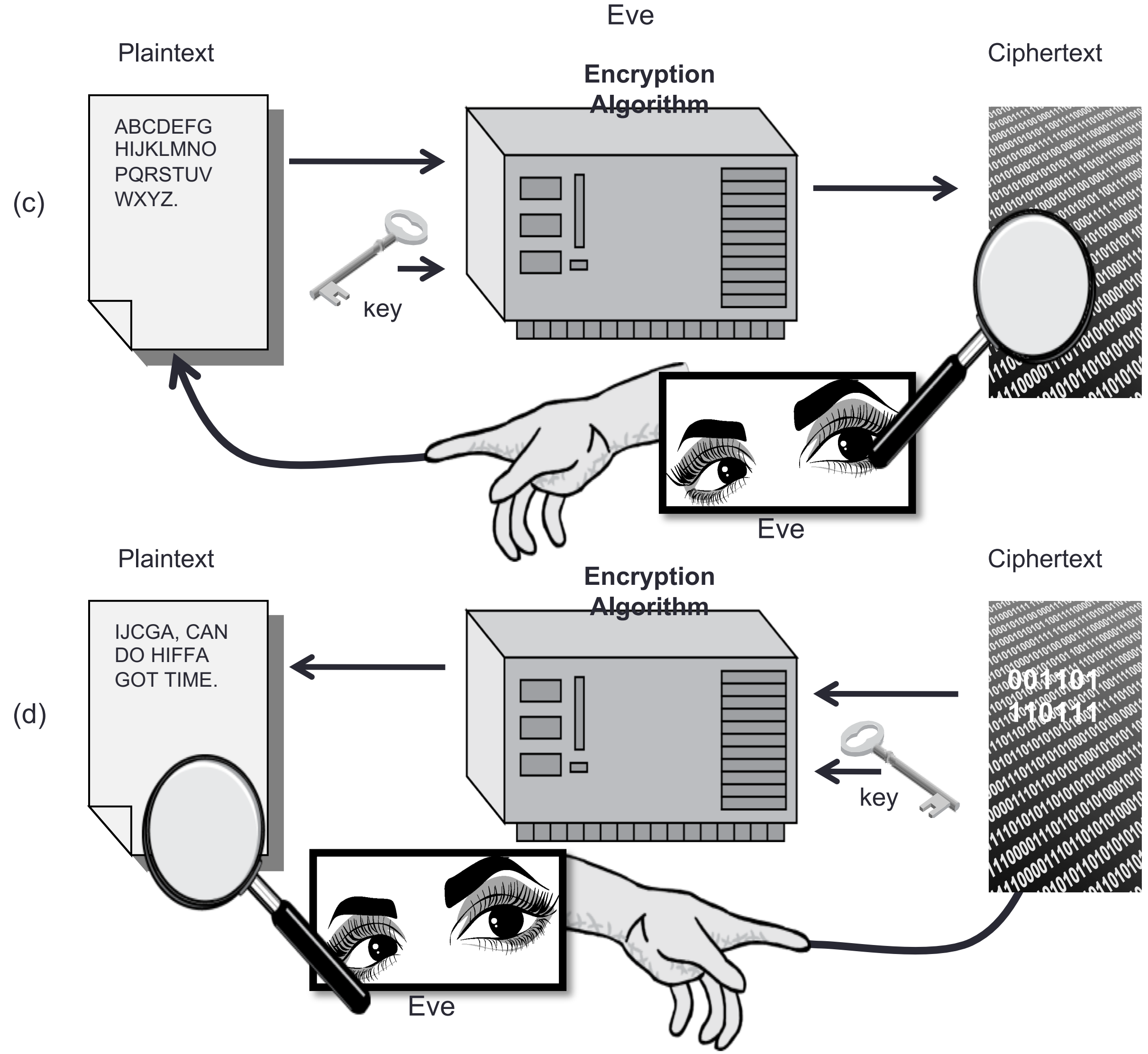


(a)
Plaintext
Hi, Bob.
Don't invite Eve
to the party!
Love, Alice
key
Encryption
Algorithm
Ciphertext
Eve
(b)
Plaintext
Hi, Bob.
Don't invite Eve
to the party!
Love, Alice
key
Encryption
Algorithm
Ciphertext
Eve

Attacks

- Attacker may have
  - collection of plaintext/ciphertext pairs for plaintexts selected by the attacker (***chosen plaintext attack***)
  - collection of plaintext/ciphertext pairs for ciphertexts selected by the attacker (***chosen ciphertext attack***)

Attacks



Cryptography

Cryptographic Primitives

- Substitution
  - One set of bits is exchanged for another
    - For example, each alphabetic letter replaced with another
    - Can also be done on data bytes or blocks
    - Involves a lookup table
      - Can be done quickly
        - Using software or optimized hardware
- Transposition
  - Rearranging the order of the ciphertext to break any repeating patterns in the underlying plaintext

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

Cryptographic Primitives

- Confusion
  - Good confusion: algorithm has a complex functional relationship between plaintext/key pair and ciphertext
    - => 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
    - => even small changes to the plaintext result in broad changes to the ciphertext

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

Cryptographic Primitives

- These are the basic techniques that make up cryptographic algorithms
- The first two—substitution and transposition—are simple mathematical operations
  - used within complex cryptosystems.
- The latter two—confusion and diffusion—are more conceptual
  - may be accomplished in a number of different ways depending on the cryptographic algorithm.

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

One-time Pad

- A one-time pad is often used as an example of the perfect cipher
- Only useful as a concept
  - completely impractical.

.

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

One-time Pad

- A one-time pad is a substitution cipher
  - Uses an arbitrarily large, nonrepeating set of keys
  - requires both an unlimited set of completely random keys and absolute sender and receiver synchronization
    - both of which are impractical.
- Resistance to cryptanalysis:
  - one-time pad is the gold standard against which other enc. algorithms are measured
    - offers no patterns for attackers to analyze.

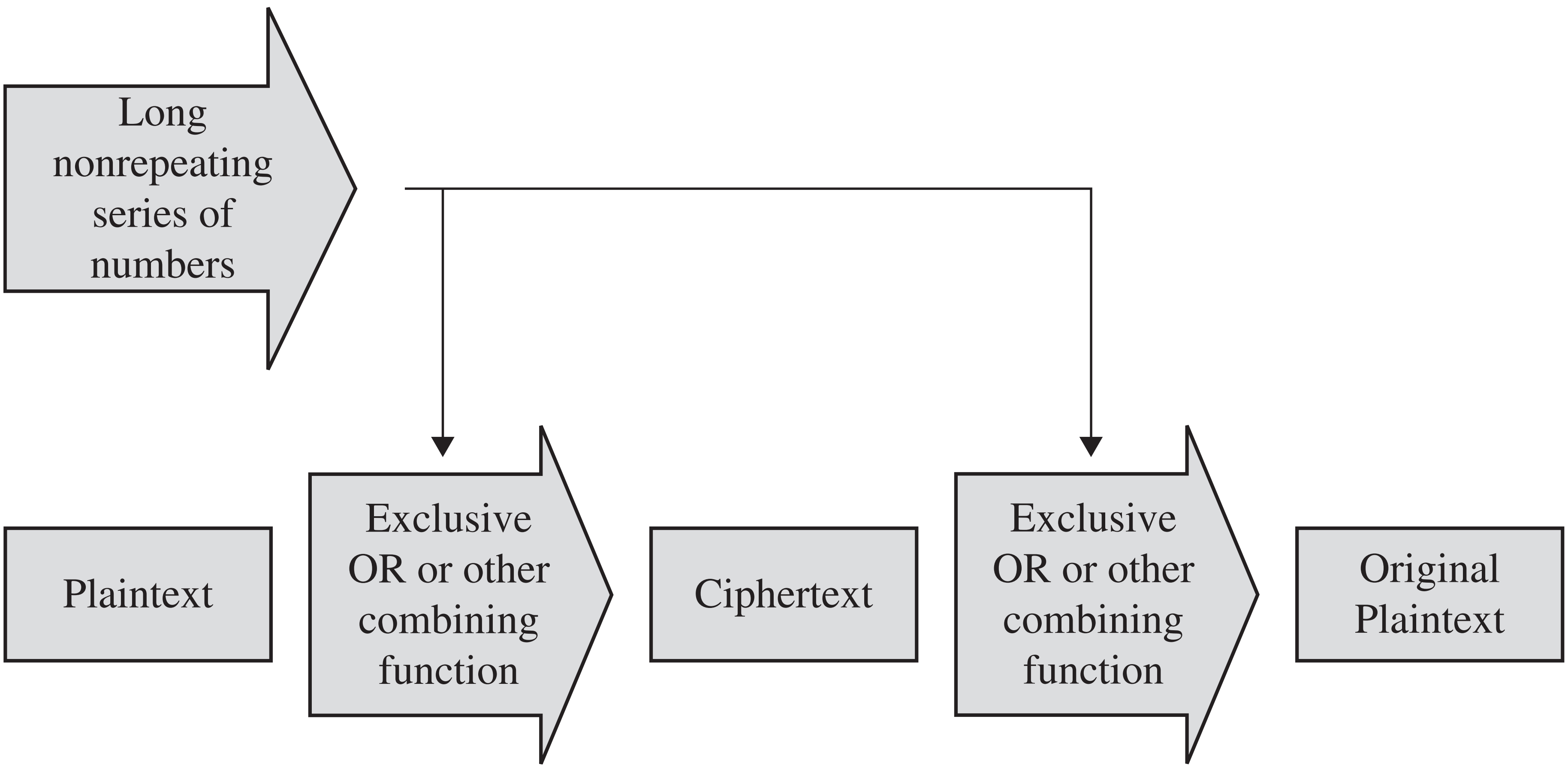
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

One-time Pad – Vernam Cipher

- Vernam cipher, a type of one-time pad
- In the Vernam cipher, XOR is used instead of pure substitution

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

One-Time Pads – Vernam Cipher



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

Shannon's Characteristics of Good Ciphers

- The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption
- The set of keys and the enciphering algorithm should be free from complexity
- The implementation of the process should be as simple as possible

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

Shannon's Characteristics of Good Ciphers

- Errors in ciphering should not propagate and cause corruption of further information in the message
- The size of the enciphered text should be no larger than the text of the original message

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

Shannon's Characteristics of Good Ciphers

- The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption
  - The degree of secrecy required factors such as key length and number of rounds
    - should be based on implementation of the algorithm, current and predicted speeds of computers, and resources of likely attackers

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

Shannon's Characteristics of Good Ciphers

- The set of keys and the enciphering algorithm should be free from complexity
  - The process has to work on any kind of plaintext input, and keys should be easy for users to generate, transmit, and store

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

Shannon's Characteristics of Good Ciphers

- The implementation of the process should be as simple as possible
  - complexity is the enemy of good security analysis.
  - It is easier to identify flaws in, and to correctly implement, a simpler algorithm
    - a simpler algorithm is therefore more likely to be free of flaws

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

Shannon's Characteristics of Good Ciphers

- Errors in ciphering should not propagate and cause corruption of further information in the message
  - Communication errors do happen, and when they do, the need for retransmission should be as limited as possible

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

Shannon's Characteristics of Good Ciphers

- The size of the enciphered text should be no larger than the text of the original message
  - A ciphertext that expands in size cannot possibly carry more information than the source plaintext
    - yet gives the cryptanalyst more data from which to infer a pattern
  - Larger messages also require more transmission time and storage and are therefore less practical for users

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

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

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

Properties of a Trustworthy Cryptosystem

- Good cryptographic algorithms are derived from sound principles and have security properties that are proven by expert mathematicians.
- Historically, algorithms that have not met this standard have been easily broken.
- Because cryptographic algorithms are complex, it can take years of analysis
  - before serious flaws are identified

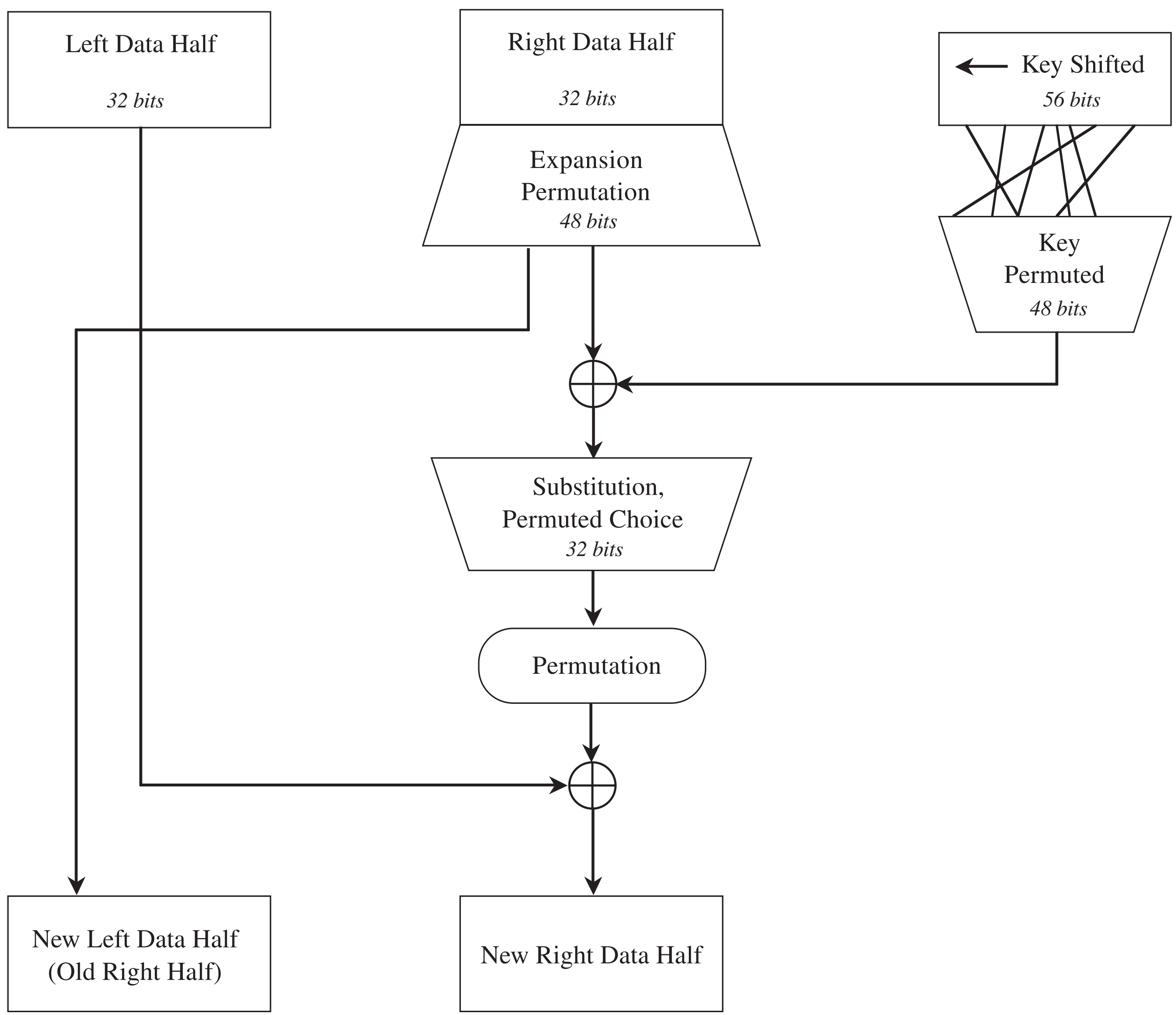
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DES Algorithm

- Symmetric cryptography algorithm
- No longer practical for use against modern technology
  - However, algorithm has a combination of strong fundamentals and relative simplicity
    - useful for demonstrating how symmetric encryption works

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

DES Algorithm – Single Cycle



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

DES Algorithm – Single Cycle

- Input to DES is divided into blocks of 64 bits
- The data bits are permuted by an "initial permutation"
- The key is reduced from 64 bits to 56 bits
  - parity bits are removed)
- The 64 permuted data bits are broken into a left half and right half
- The 32-bit right half is expanded to 58 bits
  - by repeating certain bits

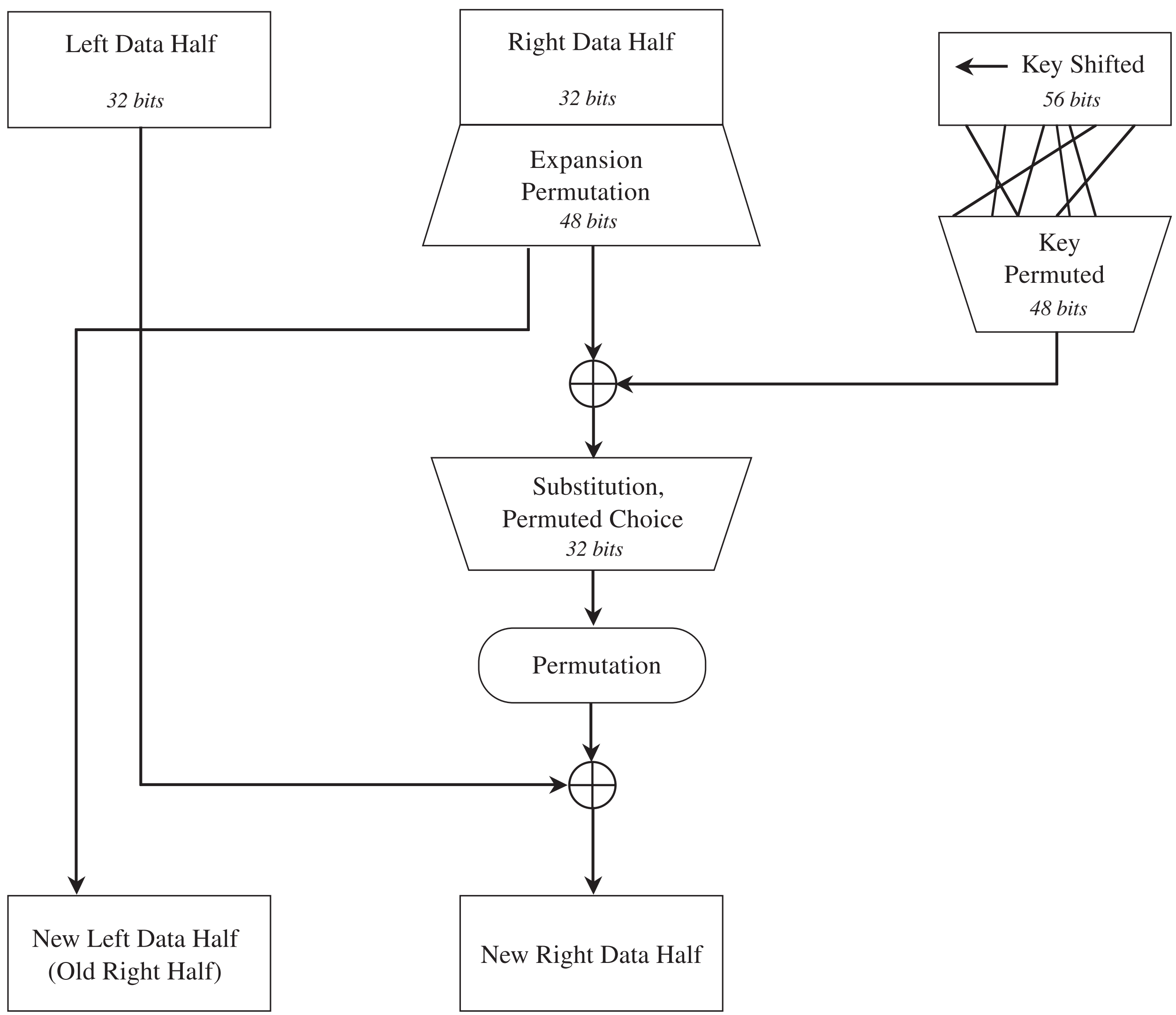
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DES Algorithm – Single Cycle (cont.)

- The key is reduced to 48 bits
  - by choosing only certain bits according to tables called S-boxes
- The key is shifted left by a number of bits and also permuted
- The key is combined with the right half, which is then combined with the left half
- The result of these combinations becomes the new right half
  - while the old right half becomes the new left half

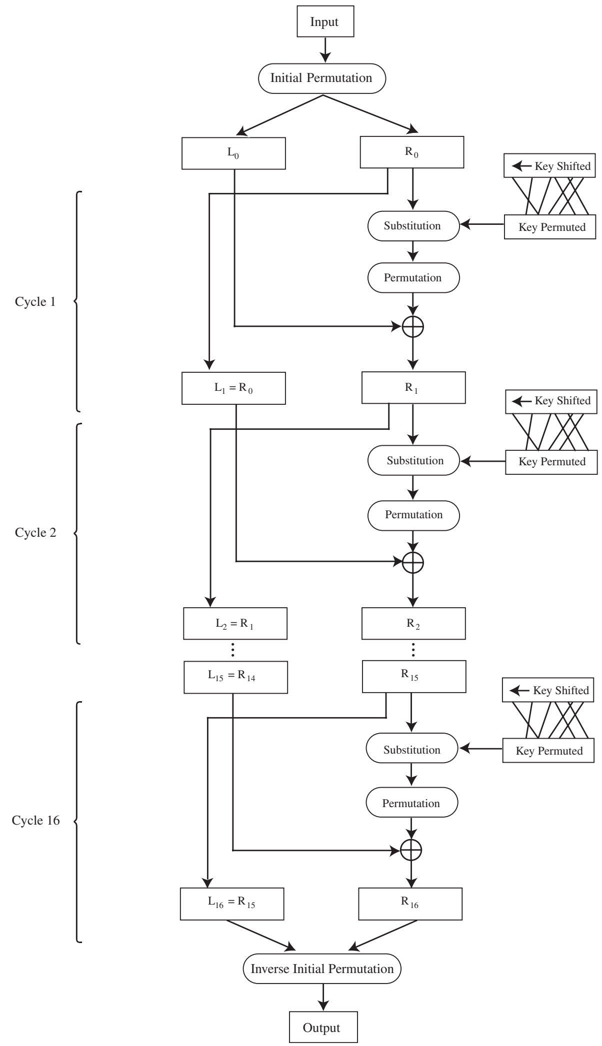
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DES Algorithm – Single Cycle



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

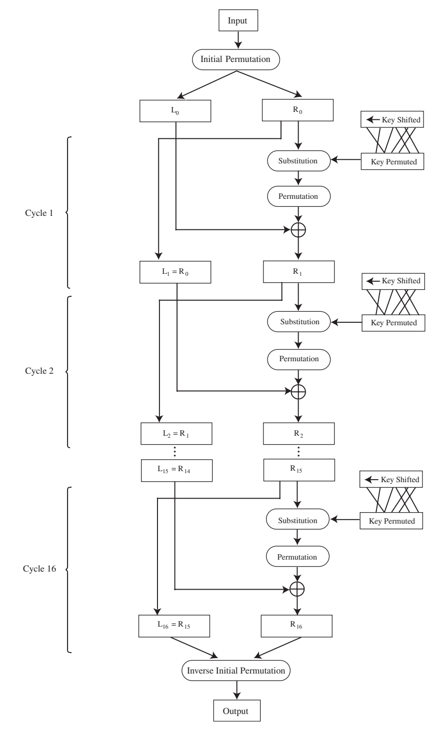
DES Algorithm (cont.)



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

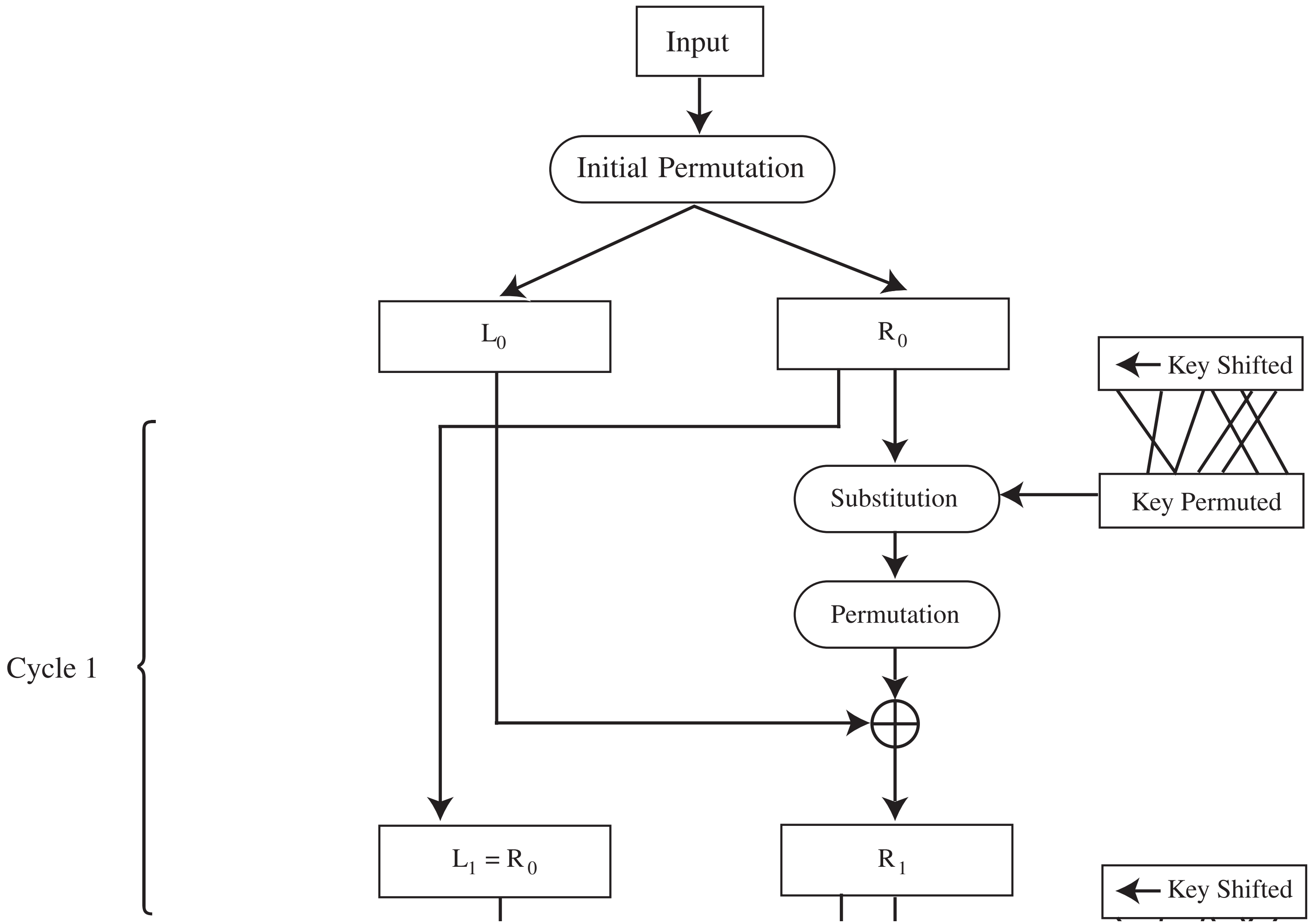
DES Algorithm (cont.)

three cycles along with the initial permutation and the final permutation:



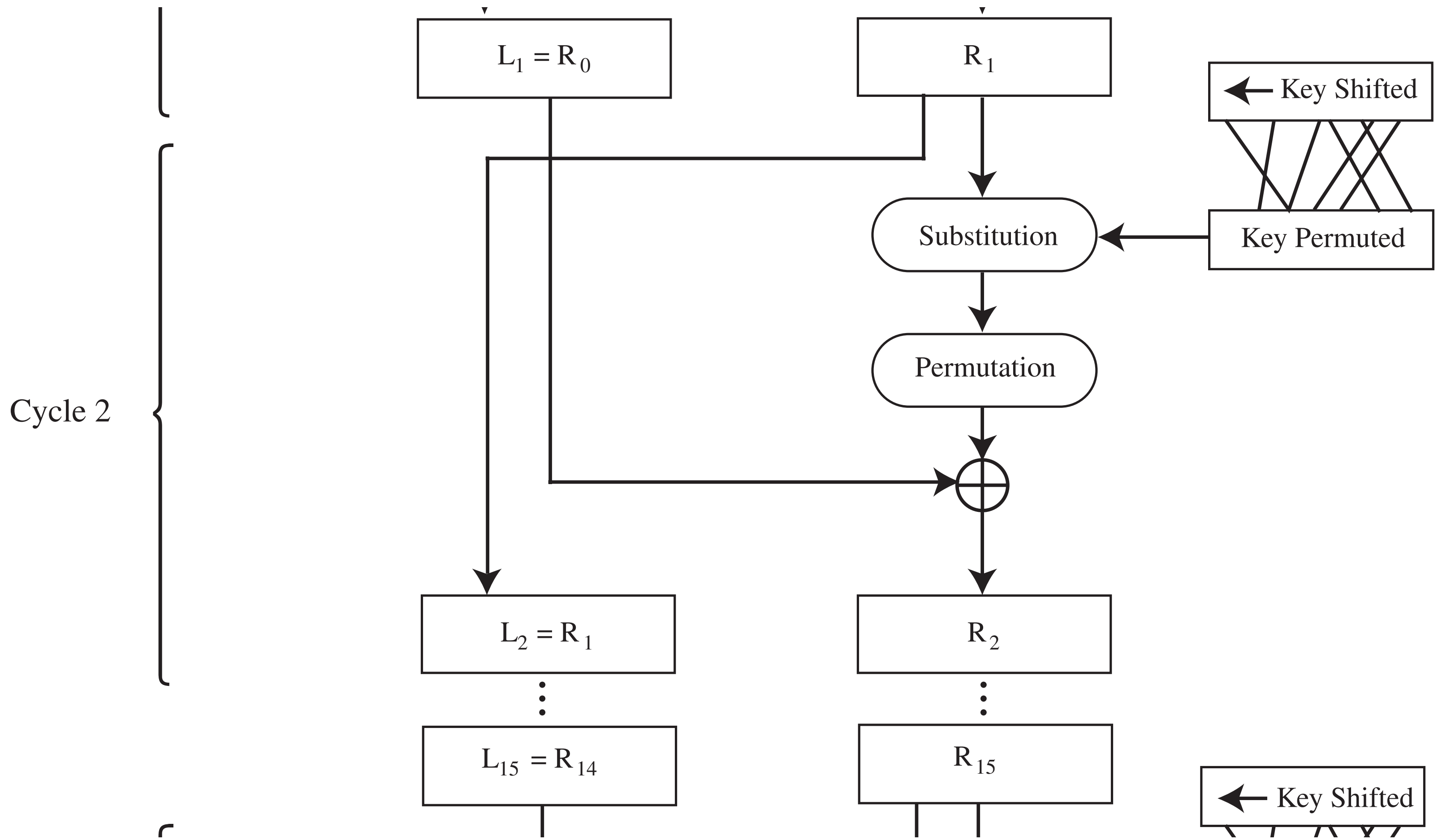
From Security in Computing, Fifth Edition, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DES Algorithm (cont.) – initial permutation



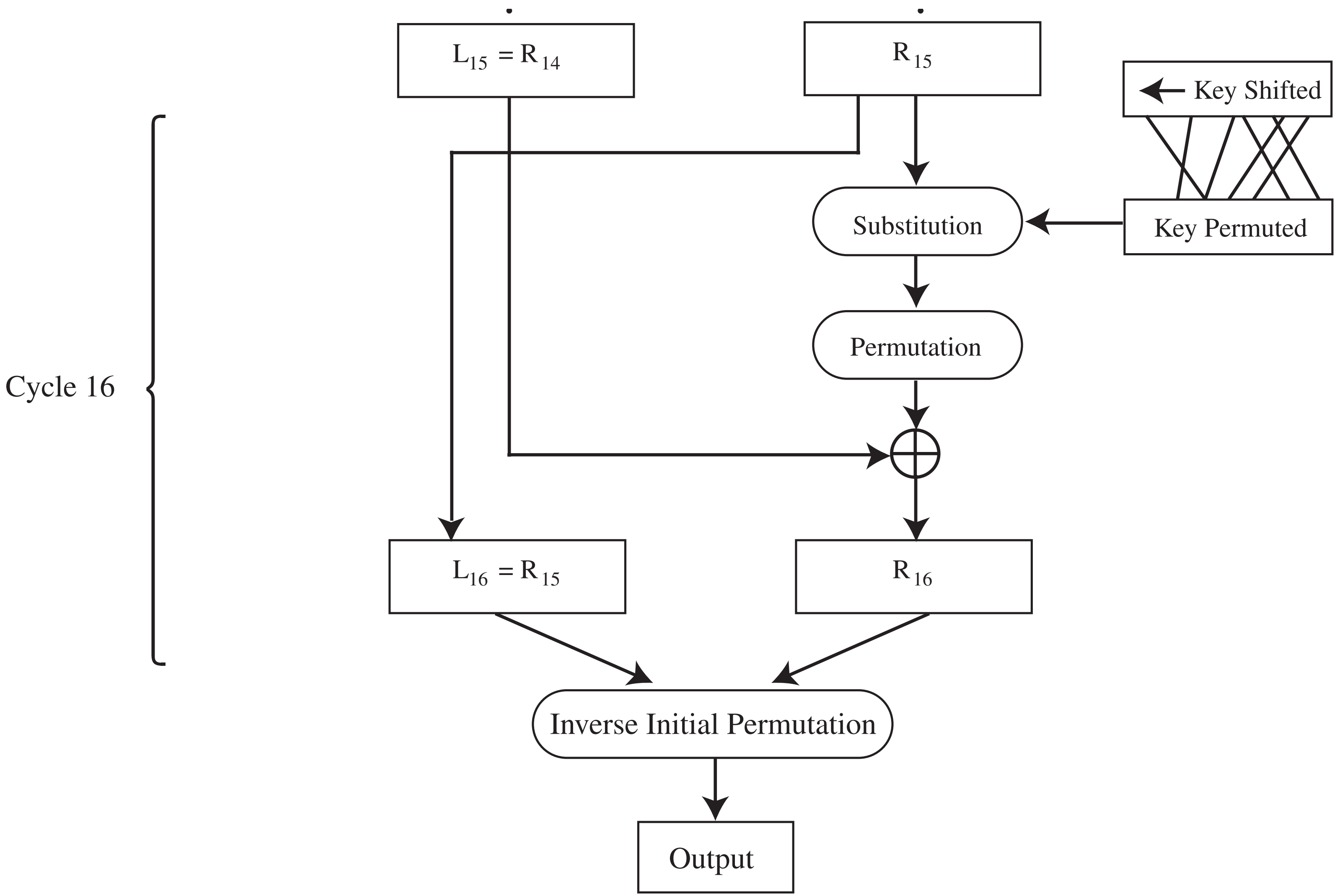
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DES Algorithm (cont.) – Single Cycle



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

DES Algorithm (cont.) – Final Permutation



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

DES Decryption

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

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

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

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

and

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

Substituting (3) into (4) gives

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

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

DES Decryption

- a single algorithm is used for both encryption and decryption.
  - L is the left-half input
  - R is the right-half input
  - *j* is the current cycle
  - *k* is the key for the current cycle
  - *f* is the function computed in an expand-shift-substitute-permute cycle.

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

DES Decryption

- Equations (3) and (5) show that R and L for the previous cycle can be derived entirely from R and L of the current cycle
  - demonstrating that the DES algorithm can work in reverse

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

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

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

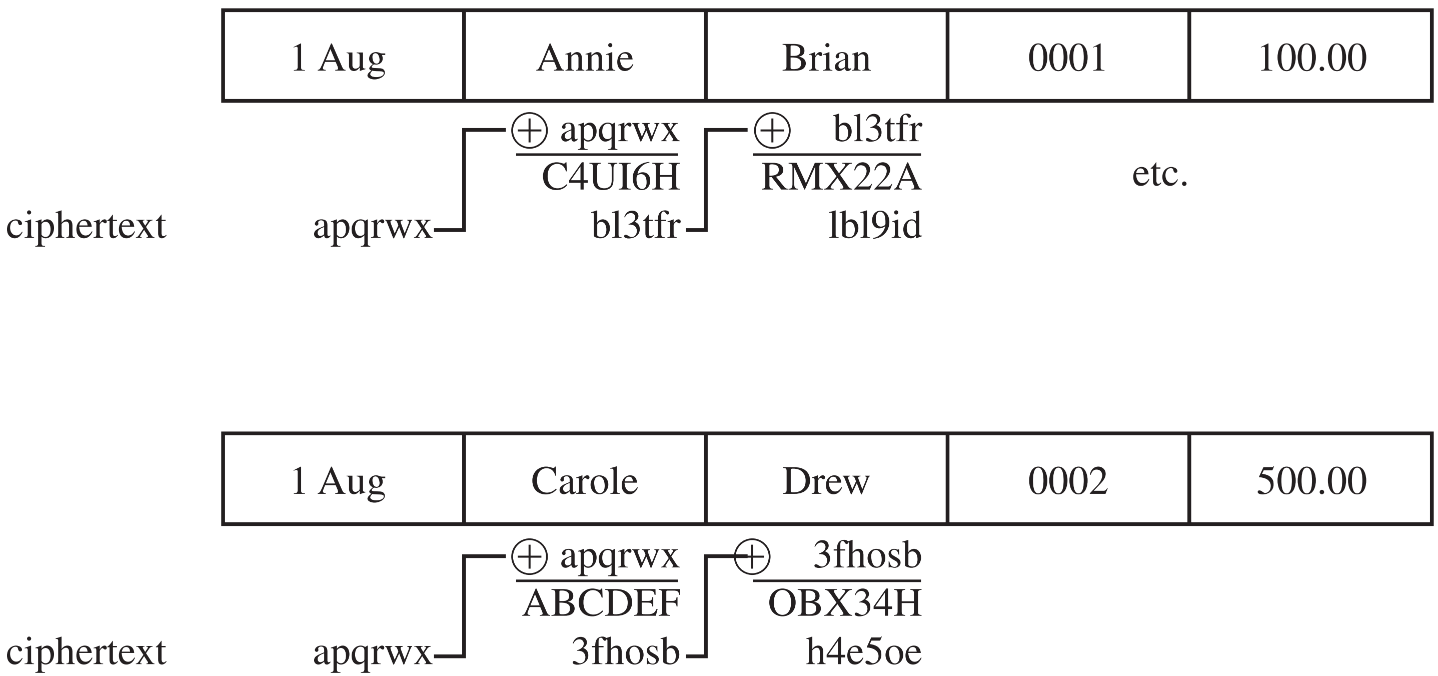
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Chaining

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

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

Simple Chaining Example



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

Simple Chaining Example

- the input of the second block is an XOR of the output of the first block and the plaintext of the second block.
- This has the effect of making identical plaintext in two different messages produce completely different ciphertext.
- But what about the first block?

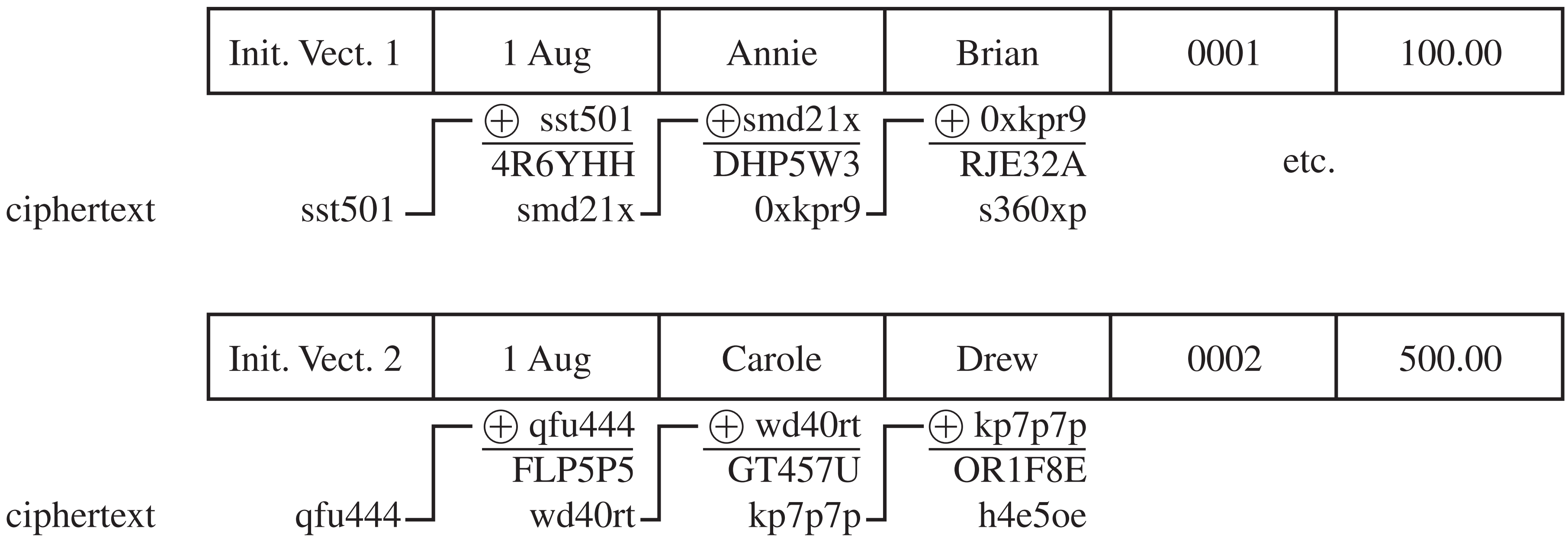
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Initialization Vectors

- To protect against the problem of identical first blocks, we start with an initialization vector:
  - an unpredictable (usually random) value that changes for each message
  - => the positive effect of chaining can be useful even for the first block of data

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

Initialization Vectors



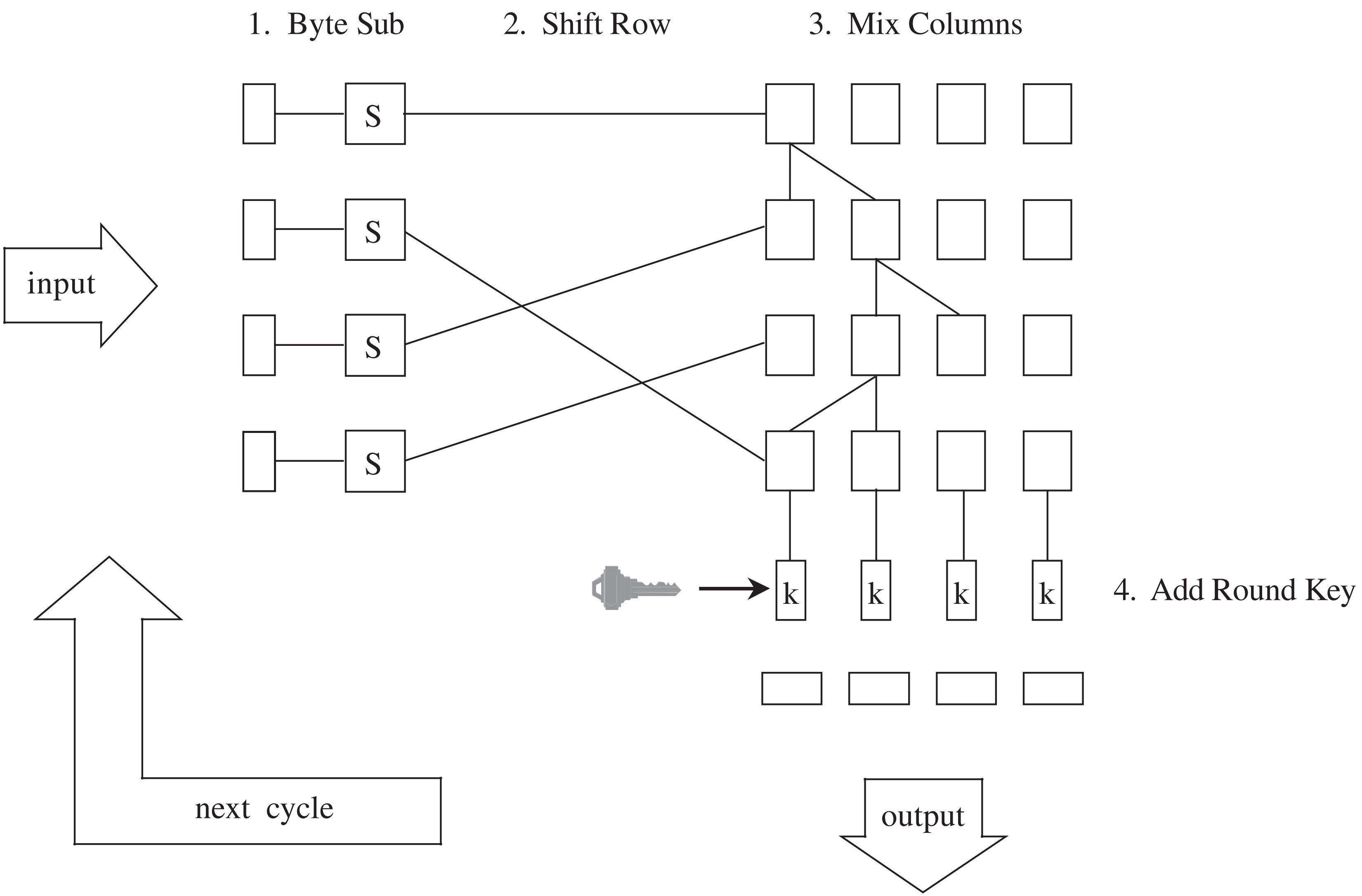
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

AES

- Symmetric cryptography algorithm
- Successor of DES
- Still considered secure

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

Structure of AES



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

Structure of AES

- AES is much more complex than DES
- The algorithm consists of 10, 12, or 14 cycles, for a 128-, 192-, or 256-bit key, respectively.
- Each cycle consists of four steps:
  - Byte substitution, shift row, mix column and add subkey
- Each cycle performs both confusion and diffusion as well as blends the key into the result

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

Structure of AES

- Byte substitution.
  - This step substitutes each byte of a 128-bit block according to a substitution table.
    - This is a straight diffusion operation.
- Shift row.
  - Certain bits are shifted to other positions.
    - This is a straight confusion operation.

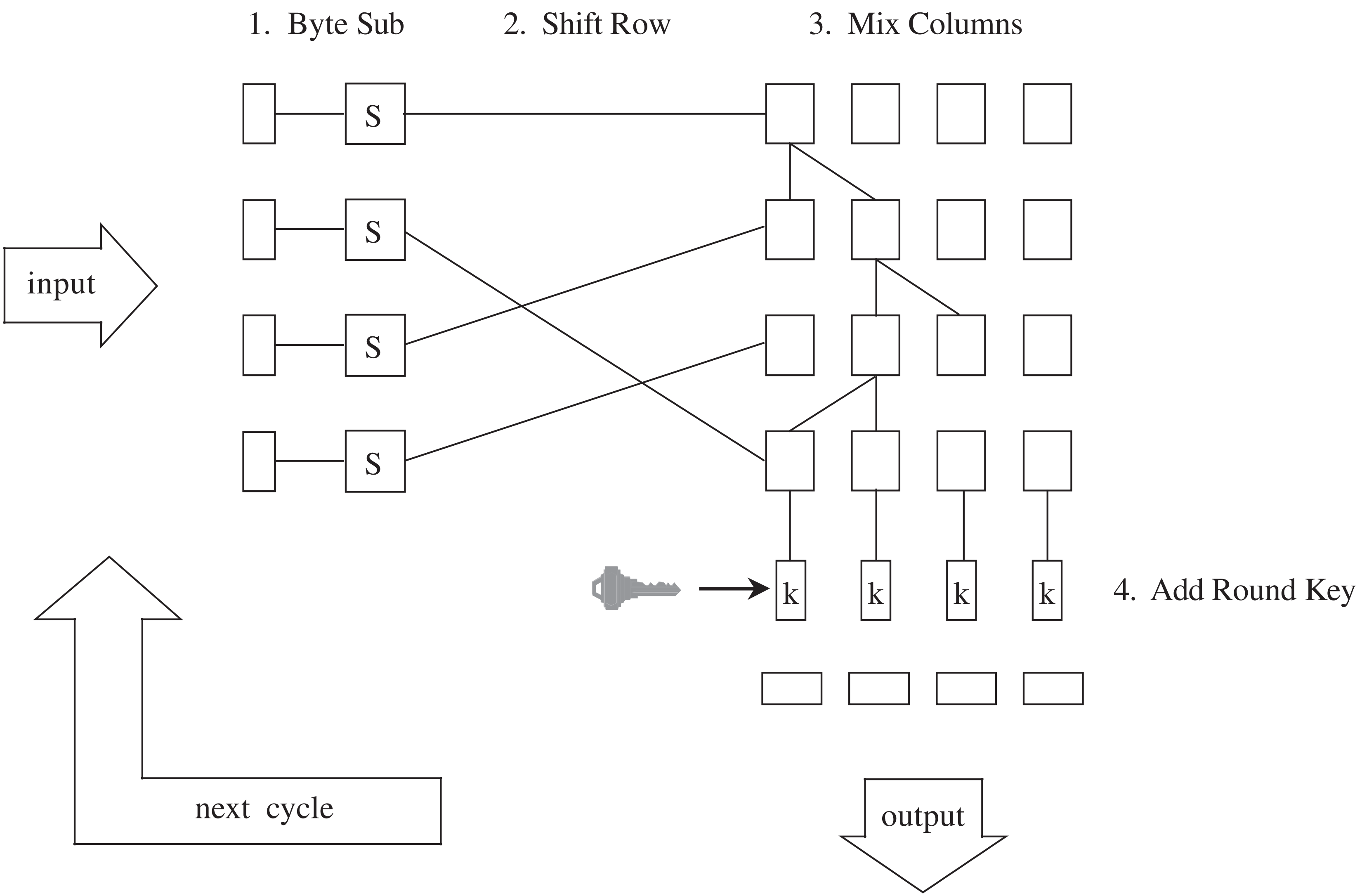
From Security in Computing, Fifth Edition, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Structure of AES

- Mix column.
  - This step involves shifting left and XORing bits with themselves.
    - These operations deliver both confusion and diffusion.
- Add subkey.
  - Here, a portion of the key unique to this cycle is XORed with the cycle result.
    - This operation delivers confusion and incorporates the key.

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

Structure of AES



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

Longevity of AES

- Since its initial publication in 1997, AES has been extensively analyzed
  - the only serious challenges to its security have been highly specialized and theoretical
- 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

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

Additional Ciphers

- RC2, RC4, RC5, and RC6 were created by Ron Rivest
  - Creator of RSA

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

RC2

- RC2 is a block cipher
  - Uses a small 40 key size
  - Intended for international use by the Lotus Notes office application suite; it would use a
    - Short enough key to satisfy U.S. export restrictions to most countries
      - thereby assuring Lotus of international marketability
    - The export of cryptographic technology from the U.S. was severely restricted by law until 1992
      - gradually eased until 2000, some restrictions still remain

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

RC2

- RC2 consists of two operations:
  - mixing and mashing.
- In mixing, a bit stream undergoes bit shifting with concurrent substitution
  - through binary (AND, OR, NOT) operations on parts of the bits.
  - During each mixing roun, a complete shuffle of bits occurs
    - from right, moving left, and cycling around to the right again.
  - There are sixteen rounds of mixing.

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

RC2

- RC2 consists of two operations:
  - mixing and mashing.
- The mashing round is pure substitution.
- No serious weaknesses have been discovered
  - but the 40-bit key makes brute-force key searches trivial

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

RC4

- RC4 is a stream cipher, widely used in wireless networks
  - WEP and WPA as well as in SSL
    - and various other products.
- RC4 was especially popular before 2000
  - like RC2, it employs a variable length key
  - => could be configured to use a 40-bit key
    - short enough to pass export restrictions

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

RC4

- RC4 is essentially a keyed pseudorandom number generator (PRNG)
  - generates a stream of bits in no predictable order.
- For encryption, the stream of bits is XORed with the plaintext bits

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

RC4

- Rc4 uses a 256-element array A containing each of the 256 possible values of an 8-bit byte
- Pointers i & j identify array bytes to be swapped.
- At each step:
  - i is incremented by 1
  - j is replaced by j + A[i]
  - A[i] and A[j] are swapped
  - byte A[A[i]+A[j]] is produced as output.

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

RC4

- The algorithm is very efficient, especially for a software implementation
- No serious cryptanalytic weaknesses have been found in the algorithm itself.
  - However the random number sequence of an XOR stream cipher must never repeat
  - => Many implementations use it with an initialization vector (IV)
    - also called a ***nonce***

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

RC5

- More complex block cipher
- A data block is split in half:
  - the left half is modified
  - the halves are swapped,
  - The new left half (that is, the old right half) is modified the same way
  - the halves are swapped again.
- That sequence constitutes a full round of the algorithm.

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

RC5

- The modifications of each half-round involve XOR, circular shift, and addition of a portion of the key.
- The number of shifted bits depends on input data:
  - The left half is shifted by the number of bits of the value of the right half.
    - Unusual for cryptographic protocols
- No significant weaknesses have been found
  - Served as a model for AES

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

RC6

- RC6 is a lightly modified version of RC5
  - a proprietary product of RSA Security
    - Does not appear to be supported

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

Key Exchange

- Reminder: for symmetric encryption, a shared secret key is needed between each two parties
- For n parties, $(0.5 \ * n \ * \ n - 1) = \ O(N^2)$ keys are needed

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

Key Exchange

- Is there a more efficient method?
  - Yes, using a third trusted party
- In this case, each party will have one shared secret key with the third trusted party
  - $K_a, K_b, k_c, etc.$

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

Key Exchange with TTP

- What A and B want to exchange a secret key:
  - TTP picks a new secret key $K_{a,b}$
  - TTP encrypts $K_{a,b}$ with K_a and sends it to A
  - TTP encrypts $K_{a,b}$ with K_b and sends it to B
  - A and B each decrypts their respective keys
    - Using their pre-shared secret key

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

Key Exchange with TTP

- Disadvantage: TTP always has to be available online to perform key exchange
- Is there another method?
  - Yes, using asymmetric encryption

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

Key Exchange with Assymetric Cryptography

- Alice chooses a pair of public and private keys K_{pb} and k_{pr}
- Alice distributes K_{pb} public key to all parties
- Bob chooses a secret key $K_{b,a}$ and encrypts it with K_{pb}
  - Sends $E\left(K_{b,a}, K_{pb}\right)$ to Alice
- Alice uses her secret key K_{pr} to decrypt $K_{b,a}$
- Alice and Bob now share a secret key $K_{b,a}$

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

Asymmetric Encryption with RSA

- RSA is an Asymmetric Encryption Algorithm
- Since its introduction in 1978, RSA has been the subject of extensive cryptanalysis
  - 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

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

Asymmetric Encryption with RSA

- Two keys, *d* and *e*, are used for decryption and encryption
  - they are interchangeable
- The plaintext block *P* is encrypted as

  $C = P^e \bmod n$
- The decrypting key *d* is chosen such that:

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

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

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.

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

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
  - A large value inhibits factoring n to infer p and q
    - but time to encrypt increases as value of n grows larger
- Typically, p and q are nearly 100 digits each
  - => n is approximately 200 decimal digits long
    - about 512 bits

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

Deriving an RSA Key Pair

- A relatively large integer *e* is chosen so that *e* is relatively prime to $(p - 1) * (q - 1)$
  - An easy way to guarantee *e* is relatively prime to $(p - 1) * (q - 1)$:
    - choose *e* as a prime that is larger than both (p − 1) and (q − 1)
- Finally, select *d* such that

$$e * d = 1\, mod\, (p - 1) * (q - 1)$$

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

RSA Example

- For example, suppose the receiver selected the primes p=11 and q=17 , along with e=3.
- The receiver calculates

$$n = p * q = 11 * 17 = 187$$

  - which is half of the public key.
- The receiver also calculates

$$f(n) = (p-1)(q-1) = 160.$$

  - e=3 was also chosen.

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

RSA Example

- For example, suppose the receiver selected the primes p=11 and q=17 , along with e=3 (cont.).
- The receiver calculates d=107, since

$$d * e = 321 = 1 \, mod \, (f(n))$$

- since The receiver distributes his public key: n=187 and e=3 .

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

RSA Example

- Now suppose the sender wanted to send the message "HELLO”
- ‘H’ is 72 in ASCII
- The sender calculates $m^e = 72^3 = 183$
  - => making the ciphertext C = 183
- The receiver calculates

  $c^d = 183^{107}$= 72 (mod 187)

  => m = 72
- Received translates message to ‘H’
- The rest of the letters are sent the same way

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

RSA Encryption

- These days, 2048-bit keys are increasingly becoming a standard requirement
  - thanks to increased computing power.
- The user of RSA distributes the value of *e* and *n* and keeps *d* secret

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

How to Break Cryptography?

- How to break cryptography

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

Message Digests

- 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

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

Message Digests

- 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

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

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

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

Digital Signatures

- Digital signatures must meet two requirements:
  - *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

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

Digital Signatures

- Digital signatures ideally satisfy two other requirements:
  - *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

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

Digital Signatures

- 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

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

Elliptic Curve Cryptosystems (ECC)

- 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 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

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

Elliptic Curve Cryptosystems (ECC)

- ECC use very complex math
- Elliptic curve cryptography is seldom used by itself for public key encryption.
- However, it is often used as a component in digital signatures

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

Elliptic Curve Cryptosystems (ECC)

- In 2005 the NSA recommended set of advanced cryptography algorithms known as Suite B.
- The protocols included in Suite B are:
  - Elliptic Curve DiffieHellman (ECDH) and Elliptic Curve Menezes-Qu-Vanstone (ECMQV) for ***key exchange***
  - The Elliptic Curve Digital Signature Algorithm (ECDSA) for ***digital signatures***
  - AES for ***symmetric encryption***
- Provides strong security, efficiency, and scalability
  - Over public-key cryptography algorithms.

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

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

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

Quantum Cryptography

- Implementations of quantum cryptography remain in the prototype stage
  - 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
  - would likely be a significant improvement over existing systems for encrypted communication

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

Quantum Cryptography

- Quantum Cryptography

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

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

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

Summary

- 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

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

Questions?

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