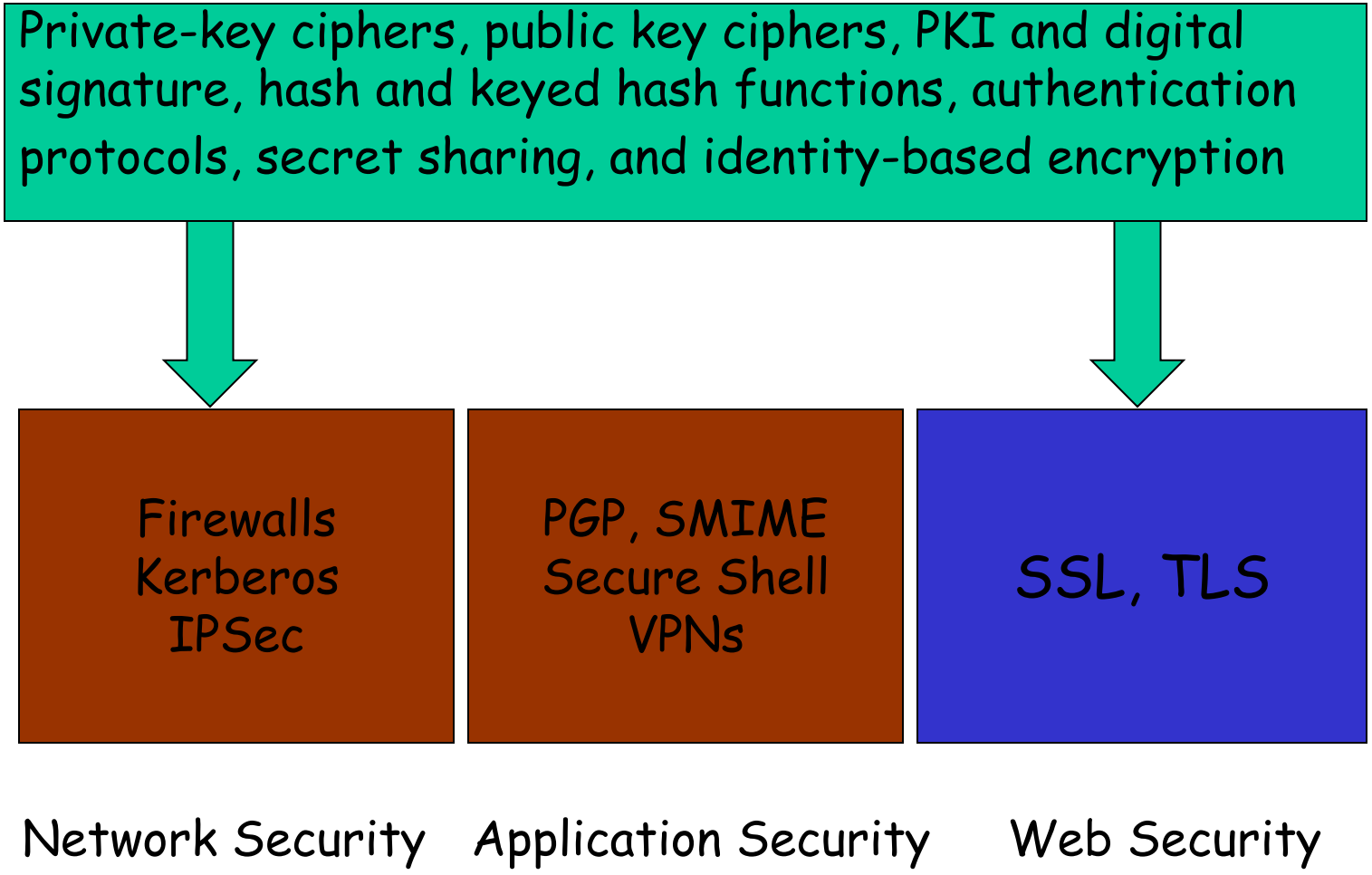
An Overview of
Cryptography and Security

Cunsheng Ding
HKUST, Hong Kong, CHINA

Cryptography



Ciphers

Data confidentiality: ciphers

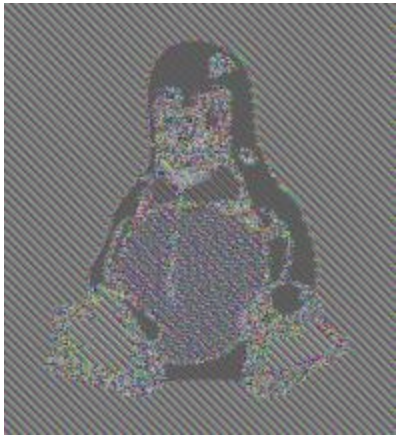
- Ciphers are classified into two types
  - One-key ciphers
  - Two-key ciphers
- Can every two-key cipher be used as public-key cipher?
- What are the main applications of public-key ciphers?

Data confidentiality: ciphers

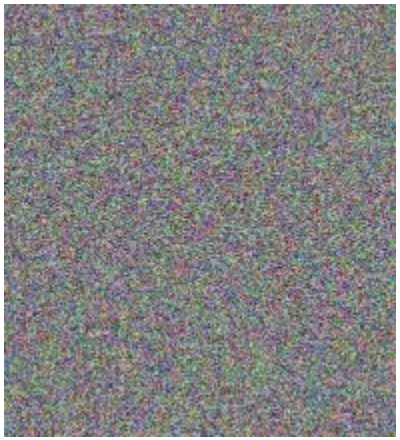
- Can every two-key cipher be used as a public-key cipher?
- What are the main applications of public-key ciphers?
  - Digital signature (nonrepudiation, sender authentication, data integrity)
  - Session key distribution
  - Mutual authentication

Data confidentiality: ciphers

Original



Encrypted using ECB mode



Encrypted using other modes

Electronic codebook (ECB), Cipher block chaining (CBC), Cipher feedback (CFB), Output feedback (OFB)

Authentication Protocols

The two most important mutual authentication protocols

- What are the two most important mutual authentication protocols introduced in this course?

The two most important mutual authentication protocols

- What are the two most important mutual authentication protocols introduced in this course?
  - Kerberos (Type-1: Windows 2000, Windows NT5)
  - Challenge-response protocol using a public-key cipher (IPSec, SSL, TLS)

Key Management

How to establish a secret number by two parties

- What are the two mostly used methods for two parties to establish a secret number?

How to establish a secret number by two parties

- What are the two mostly used methods for two parties to establish a secret number?
  - DH [DH groups] (IPSec, SSL/TLS)
  - Using a public key cipher (IPSec, SSL/TLS)

Sender Authentication + Data Integrity

The major techniques for data integrity + sender authentication

- What are the major techniques for sender authentication plus data integrity?

The major techniques for data integrity and sender authentication

- What are the major techniques for data integrity plus sender authentication?
  - Digital signature (public-key cipher) [PGP, S/MIME]
  - Message authentication codes
    - keyed hash function
    - secret key + hash function with HMAC (IPSec, SSL/TLS)

X.509 Digital Certificate

X.509 Digital Certificate

- Three versions (v.1, v.2, v3)
  - We introduced only Version 3. That is why you see different ones.
- It is used in:
  - S/MIME
  - IP Security
  - SSL/TLS
  - SET

Digital Signature

Digital Signature

- Two methods:
  - RSA+ Hash
  - DSS + Hash
- There are similarities and differences between handwritten and digital signature
- Important (nonrepudiation, sender authentication, data integrity)
- Used in PGP and S/MIME, and SSH

IP Security

IP Security

- Why do we need two modes (the transport and tunnel mode) in IP Security?

IP Security

- Why do we need two modes (the transport and tunnel mode) in IP Security?
  - There are 4 possible situations.

IP Security

- IP Security has two subprotocols, the ESP and AH. What is the purpose of having two subprotocols?

IP Security

- IP Security has two subprotocols, the ESP and AH. What is the purpose of doing this?
  - To cater with requirements of different security services.

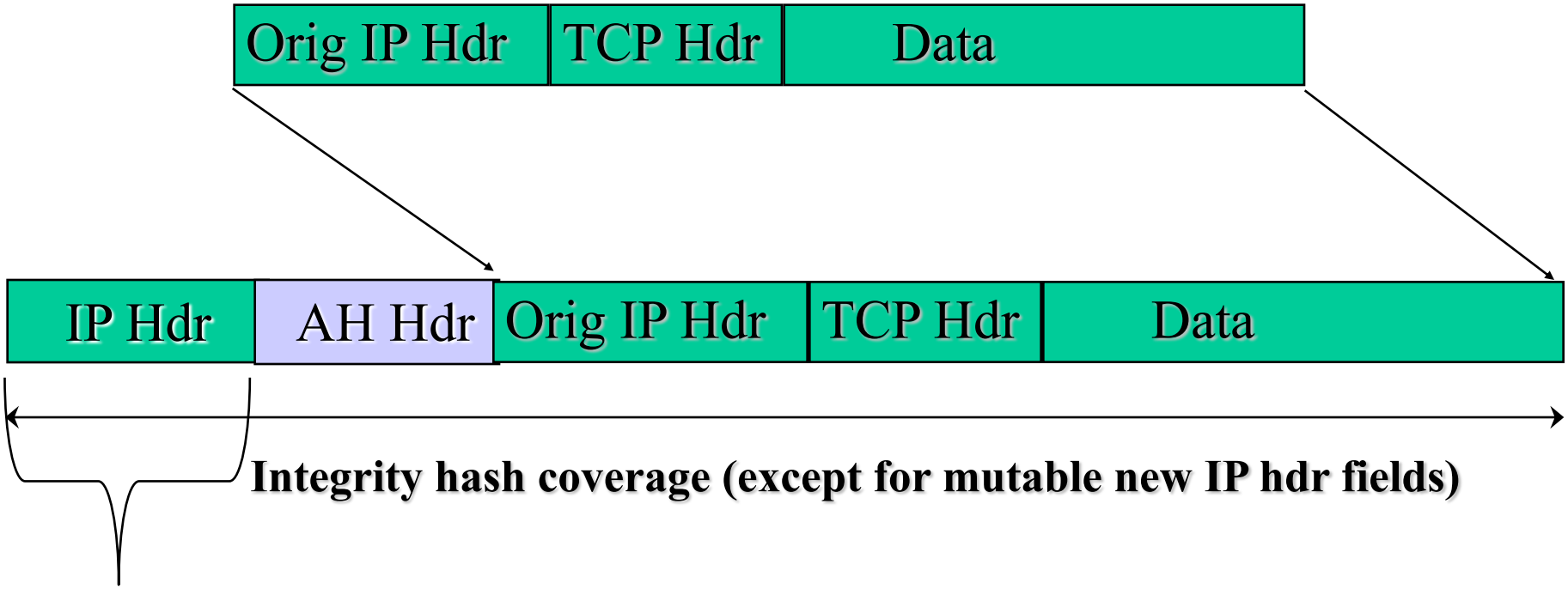
IP Security

- Can AH provide limited traffic flow confidentiality when it is used in the tunnel mode?
  - We know that this is true for the ESP.

IP Security

- Can AH provide limited traffic flow confidentiality when it is used in the tunnel mode?
  - No.
  - Even though a new IP header is inserted, the original IP header is not encrypted.

IPSec AH in Tunnel Mode



New IP header with source & destination IP address

IP Security

- IPSec has a suite of algorithms: What does "mandatory-to-implement" mean?
- What is the purpose of doing this?

IP Security

- IPSec has a suite of algorithms: What does "mandatory-to-implement" mean?
  - 3DES in CBC, SHA-1 must be supported in every IPSec module
- What is the purpose of doing this?
  - To ensure that two IPSec modules will be able to agree on a cipher and a hash function.

IP Security

- To protect the communication between two hosts, a pair of security associations are established. Each is for one direction. An alternative is that only one SA is used for protecting data in both directions. What are the advantages of the approach of IP Security?