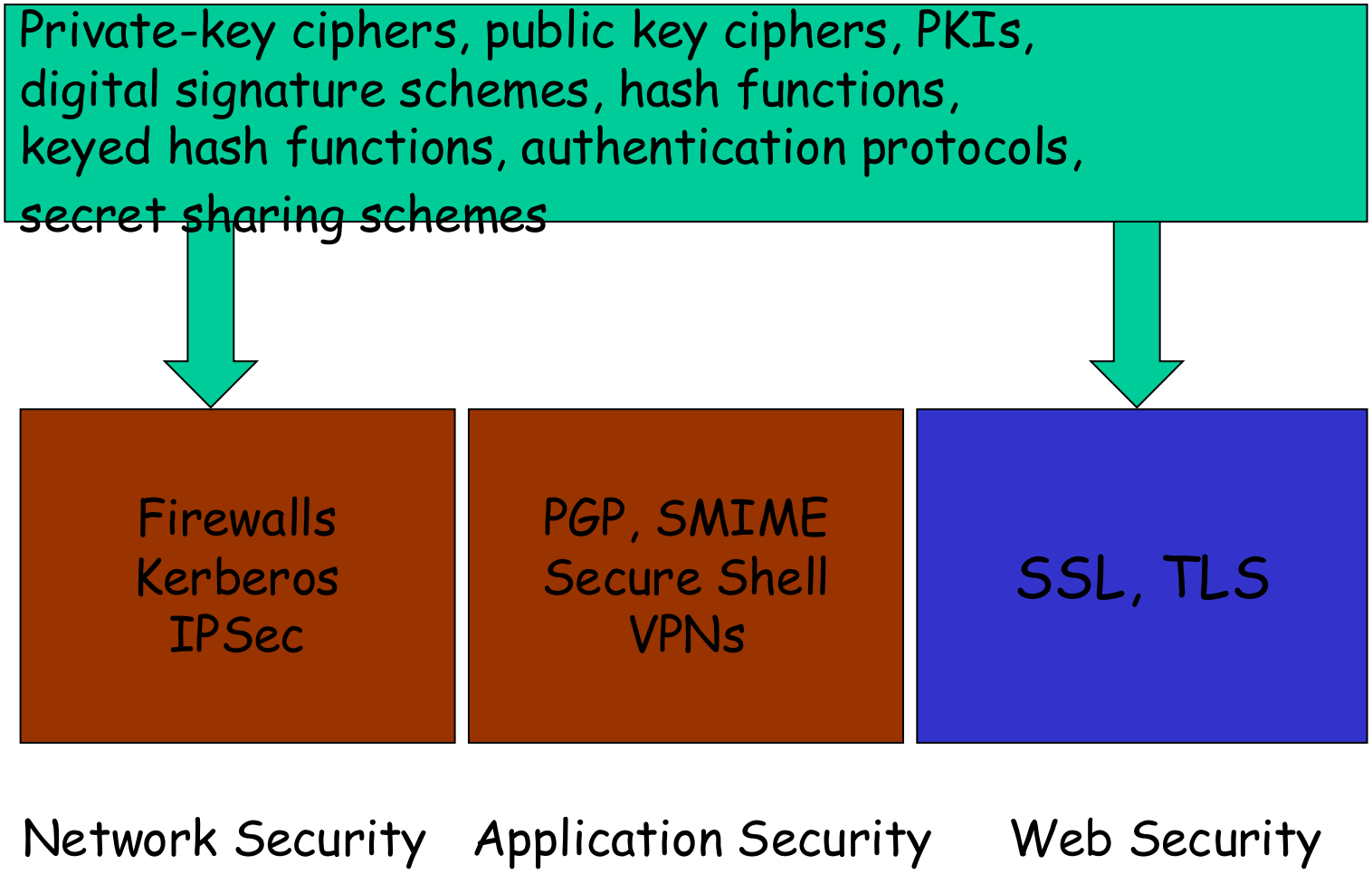
A Selective Review of COMP5631

Cunsheng Ding
HKUST, Hong Kong, CHINA

Cryptography



Ciphers

Ciphers

- Ciphers are classified into two types
  - One-key ciphers (block and stream ciphers)
  - Two-key ciphers

Ciphers

- Can every two-key cipher be used as a public-key cipher?

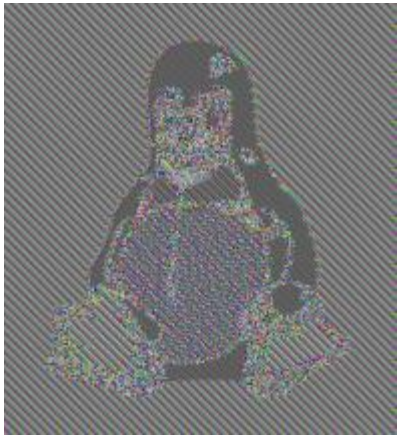
Ciphers

- What are the main applications of public-key ciphers?
  - Digital signature (signer nonrepudiation, data origin authentication, data integrity)
  - Session key distribution
  - Mutual authentication
  - User and server authentication (e.g., SSH)

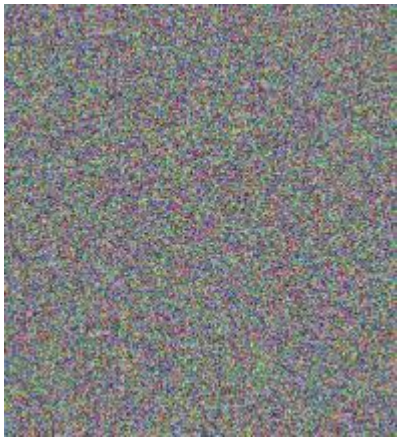
Why stream ciphers?



Original



Encrypted using ECB mode



Encrypted using other modes

Electronic codebook (ECB), Cipher block chaining (CBC), Counter mode

X.509 Digital Certificate

X.509 Digital Certificate

- Three versions (v.1, v.2, v3)
- It is used in:
  - S/MIME
  - IP Security
  - SSL/TLS
- You need to recall the necessity of having a digital certificate issued by a certificate authority.

Digital Signature Schemes

Digital Signature Schemes

- Two schemes:
  - RSA+ Hash
  - DSS
- Used in PGP and S/MIME, and SSH

Digital Signature

- There are similarities and differences between handwritten and digital signature
- Security services provided by the digital signature are the following:
  - signer nonrepudiation,
  - data origin authentication,
  - data integrity,
  - client and server authentication (e.g.,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?
  - Some computers may not have the IPSec software installed.
  - 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.

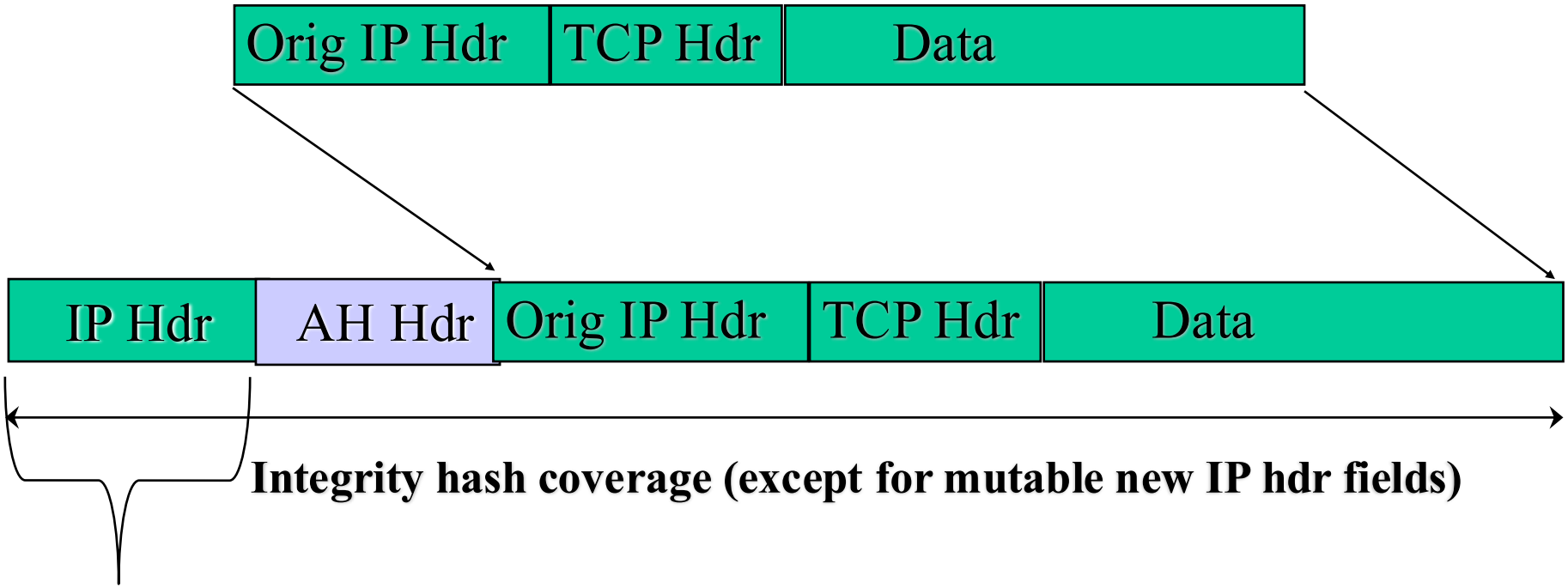
IP Security

- 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 and some of them are mandatory-to-implement. 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.