

CSE/EE 461 – Lecture 23

Network Security

David Wetherall
djw@cs.washington.edu

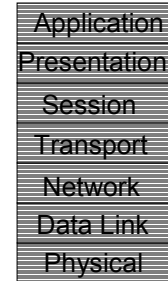
Last Time

- Naming
- Focus
 - How do we name hosts etc.?
- Topics
 - Domain Name System (DNS)
 - Email/URLs

Application
Presentation
Session
Transport
Network
Data Link
Physical

This Time

- Network security
- Focus
 - How do we secure distributed systems?
- Topics
 - Privacy, integrity, authenticity
 - Cryptography



What do we mean by "Security"?

- Networks are fundamentally shared
 - Need means to protect messages sent by legitimate participants from others with access to the network
- Privacy: messages can't be eavesdropped
- Integrity: messages can't be tampered with
- Authenticity: messages were sent by the right party
- These are in addition to the need to protect networked systems from intrusions and compromise by attackers

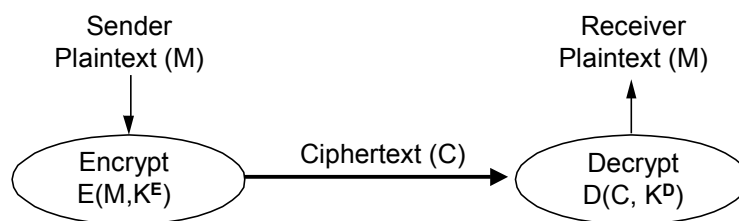
Approaches at 10,000 ft

- Physical security
 - Tackle the problem of sharing directly
- “Security through obscurity”
 - Hope no-one will find out what you’re doing!
- Throw math at the problem
 - Cryptography
- Why is security difficult?
 - It’s a negative goal: can you be sure there are no flaws?
 - Often assumptions turn out to be invalid, esp. randomness

djw // CSE/EE 461, Winter 2003

L23.5

Basic Encryption for Privacy



- Cryptographer chooses functions E , D and keys K^E , K^D
 - Mathematical basis
- Cryptanalyst try to “break” the system
 - Depends on what is known: E and D , M and C ?

djw // CSE/EE 461, Winter 2003

L23.6

Secret Key Functions (DES, IDEA)

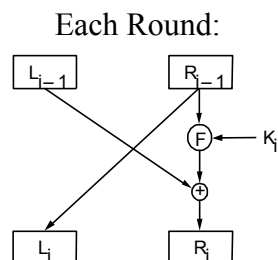
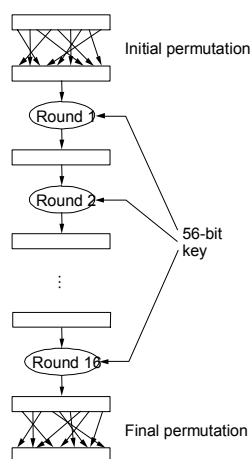


- Single key (symmetric) is shared between parties
 - Often chosen randomly, but must be communicated

djw // CSE/EE 461, Winter 2003

L23.7

Basics of DES

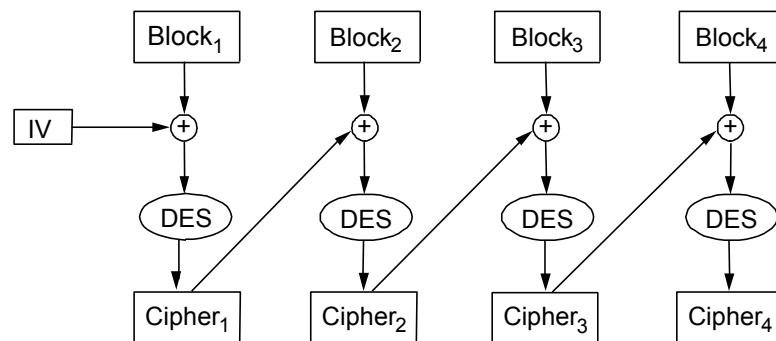


DES uses a 64 bit key (56 + 8)
Message encrypted 64 bits at a time
16 rounds in the encryption
Each round scrambles 64 bits

djw // CSE/EE 461, Winter 2003

L23.8

DES (cont.)



- Repeat process for larger messages with “chaining”

djw // CSE/EE 461, Winter 2003

L23.9

Public Key Functions (RSA)



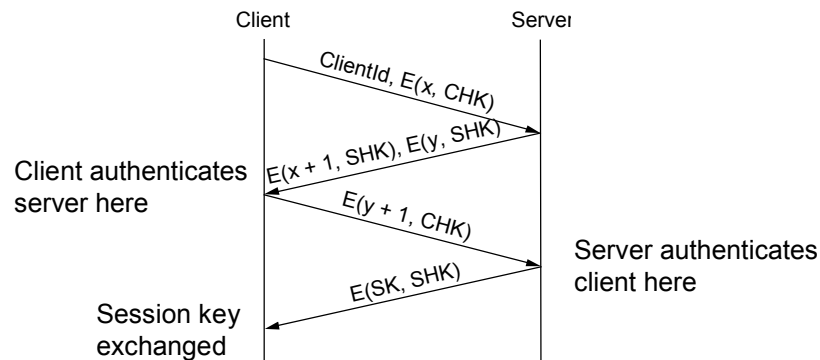
- Public and private key related mathematically
 - Public key can be published; private is a secret

djw // CSE/EE 461, Winter 2003

L23.10

Authentication Protocols

- Three-way handshake for mutual authentication
 - Client and server share secrets, e.g., login password



djw // CSE/EE 461, Winter 2003

L23.11

Authenticity and Integrity

- Sometimes we care about knowing messages authentic, but don't care about privacy.
- If only sender and receiver knew the keys we would be done ... but that's often not the case
 - A pair of keys for each pair of communicating parties?
- In public key (RSA) systems the "encryption" key is potentially known by everyone
 - anyone could have sent us a confidential message by encrypting with our public key

djw // CSE/EE 461, Winter 2003

L23.12

RSA Digital Signature



- Notice that we reversed the role of the keys (and the math just works out) so only one party can send the message but anyone can check it's authenticity

djw // CSE/EE 461, Winter 2003

L23.13

A Faster "RSA Signature"

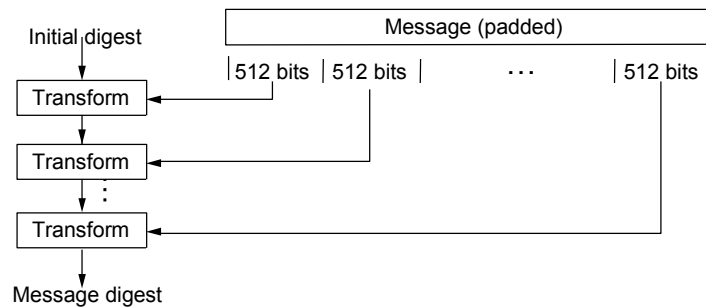
- Encryption can be expensive, e.g., RSA 1Kbps
- To speed up, let's sign just the checksum!
 - Check that the encrypted bit is a signature of the checksum
- Problem: Easy to alter data without altering checksum
- Answer: Cryptographically strong "checksums" called message digests where it's computationally difficult to choose data with a given checksum
 - But they still run much more quickly than encryption
 - MD5 (128 bits) is the most common example

djw // CSE/EE 461, Winter 2003

L23.14

Message Digests (MD5, SHA)

- Act as a cryptographic checksum or hash
 - Typically small compared to message (MD5 128 bits)
 - “One-way”: infeasible to find two messages with same digest



djw // CSE/EE 461, Winter 2003

L23.15

Cryptography in Protocols

- These techniques can be applied at different levels:
 - IP packets (IPSEC)
 - Web transfers or other transports (SSL/TLS, Secure HTTP)
 - Email (PGP)
- Next time ..

djw // CSE/EE 461, Winter 2003

L23.16

Key Concepts

- Privacy, integrity, and authenticity
- Cryptographic mechanisms are used to support these properties: private key, public key and digests