

Chapter 13

by
David G. Messerschmitt

Understanding Networked Applications:
A First Course

Trustworthiness

by
David G. Messerschmitt

Some objectives

- High availability
  - Expanding expectations, approaching 24x7
  - Redundancy/replication, security, human factors
- Protect confidential information
- Limit services to legitimate users or customers
- Conduct secure commercial transactions

Availability

- Application up and running correctly
- Some types of downtime:
  - Off-line upgrade and maintenance
  - Software crashes
  - Equipment failure
  - Successful denial-of-service attack

Availability costs!

- On-line upgrade and maintenance
- More application testing, more rapid bug reports and fixes
- Equipment or application redundancy
- Data replication
- Operational vigilance

Question

- What availability would you like to see in:
  - Consumer stock trading system?
  - Currency trading system?
  - Train control system?
  - Bank ATM?
  - Social application like email?
  - Telephone system?

Different security environments

- Intranet and extranet
  - All users may be trusted
- Organization-to-organization
  - Users in other organizations are less trusted, have less access
- Citizenry
  - Determined adversaries must be assumed

7

Access control

- First line of defense is to limit information and services to authorized users
- Requires:
  - Authorization policies
  - Databases with authorizations
  - Confidentiality of information and communication
  - Authentication of users who do gain access

8

Non-repudiation

- The second line of defense is to maintain a provable audit of commitments
  - Requires non-repudiation: neither sender nor recipient can deny message
  - Non-repudiation requires message integrity

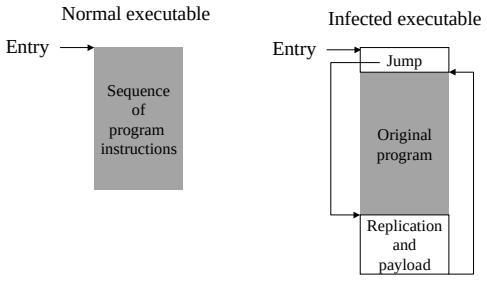
9

Core technology

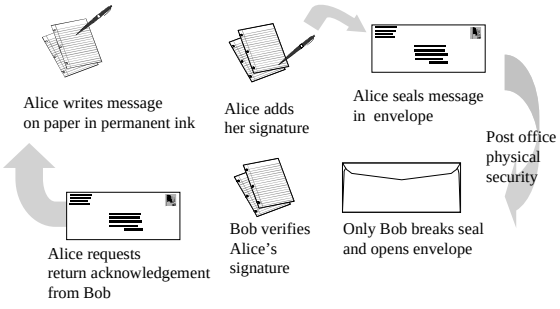
- Encryption
  - Depends on the existence of hard (not impossible) problems that are thought to be uncomputable by the fastest computers in reasonable time
  - "Size" of problem can be adjusted to future and anticipated computing technology
  - Symmetric and asymmetric versions

10

Virus



11

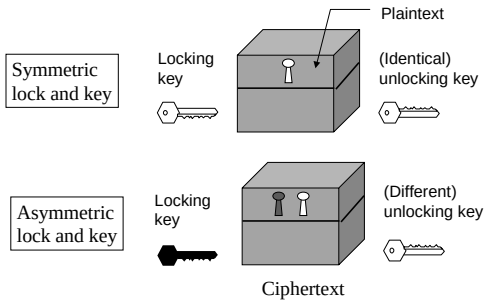


12

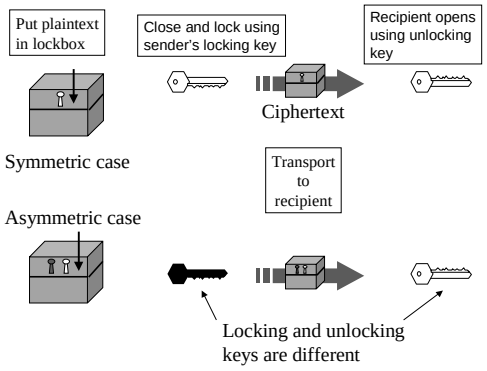
Encryption

- Transform "plaintext" data to "ciphertext" data in a way that
  - plaintext cannot be recovered without knowledge of a key
  - at least not without extraordinary computing resources

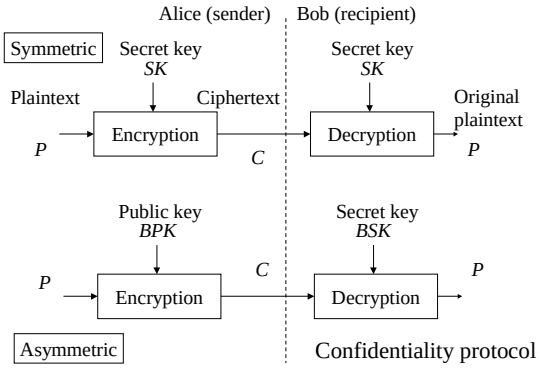
13



14

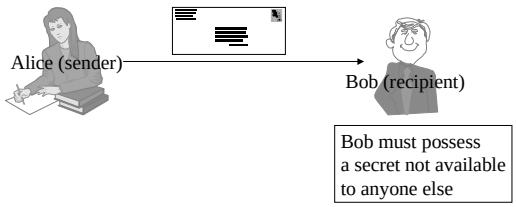


15



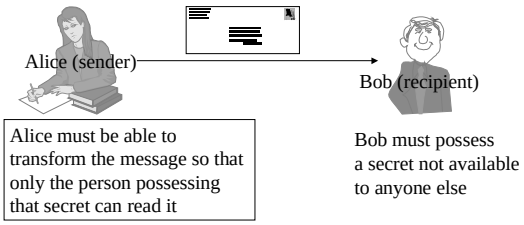
16

Confidentiality



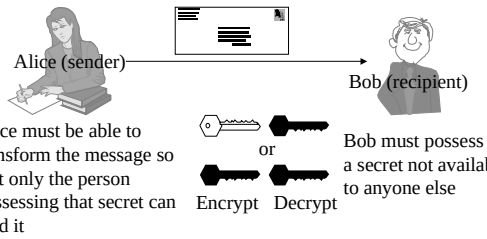
17

Confidentiality (con't)



18

Confidentiality (con't)



Alice must be able to transform the message so that only the person possessing that secret can read it

Bob must possess a secret not available to anyone else

19

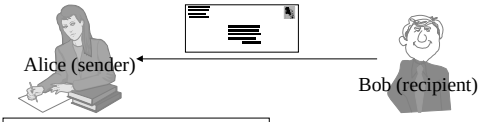
Authentication

Goal:

- Before Bob can trust a message received from Alice, he needs to verify that Alice is who she claims she is
- Alice may want to verify Bob's identity before sending him a message

20

Authentication



Alice must possess a secret not available to anyone else (alternatively, physical characteristics like a finger print might be used)

21

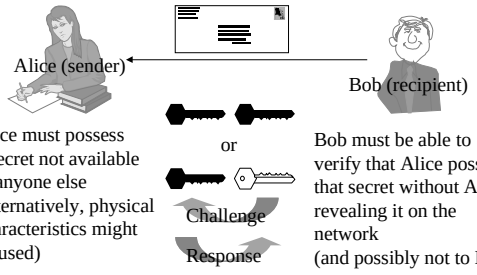
Authentication (con't)

Alice must possess a secret not available to anyone else (alternatively, physical characteristics might be used)

Bob must be able to verify that Alice possesses that secret without Alice revealing it on the network or to Bob

22

Authentication (con't)

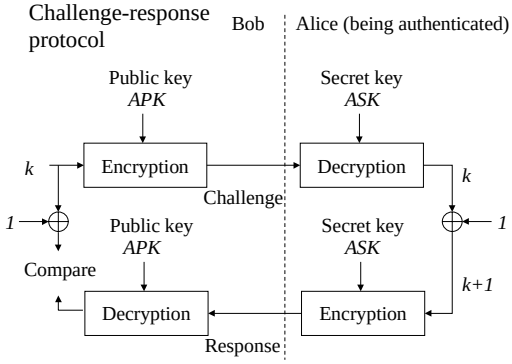


Alice must possess a secret not available to anyone else (alternatively, physical characteristics might be used)

Bob must be able to verify that Alice possesses that secret without Alice revealing it on the network (and possibly not to Bob)

23

Challenge-response protocol



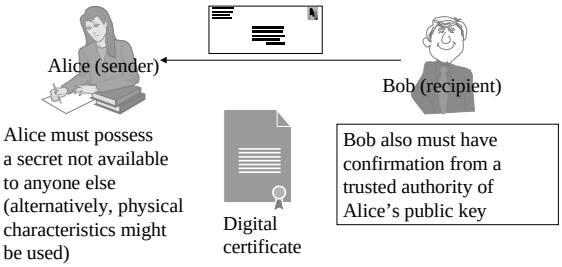
24

Question

- How does Bob obtain Alice's public key?
- How does Bob authenticate that public key?
- Answer: Key must come from a trusted authority

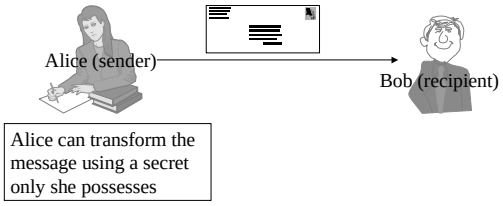
25

Authentication (con't)



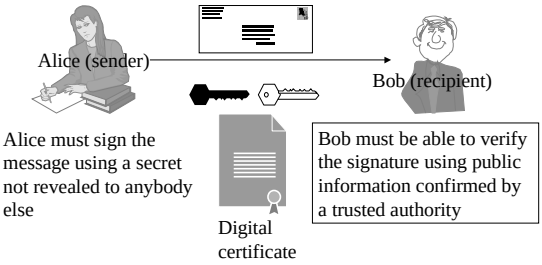
26

Non-repudiation



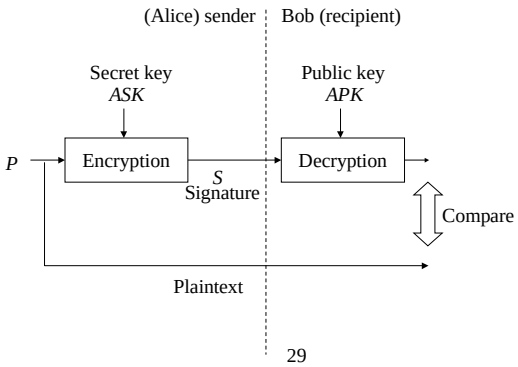
27

Non-repudiation



28

Digital signature



29

Summary

- A message can be sent from Alice to Bob, such that:
  - It is confidential
  - Alice's identity is authenticated
  - Provably the message was not modified after Alice generated it, and she cannot repudiate it
- All this requires a system for distribution and certification of secrets

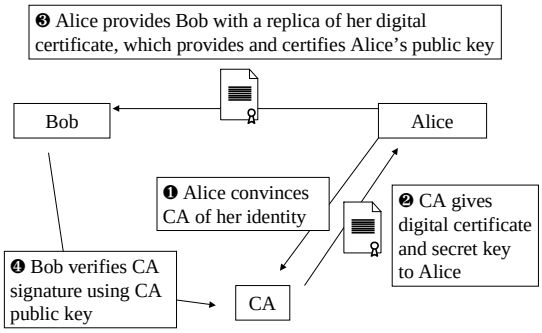
30

Distribution of secrets

- Users choose their own secrets and inform sites (password)
- In a closed administrative environment, secrets can be distributed by administrative fiat
  - Authentication servers avoid the "n^2 secret problem"
- For the citizenry, infrastructure required

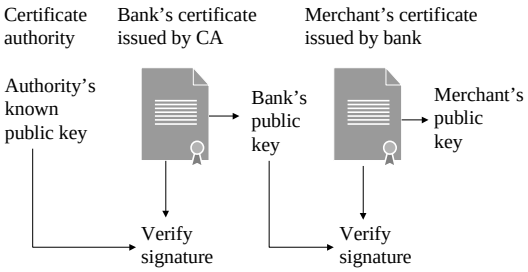
31

Digital certificate protocol



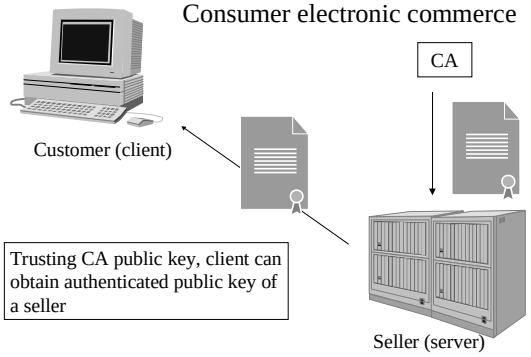
32

Chain of trust

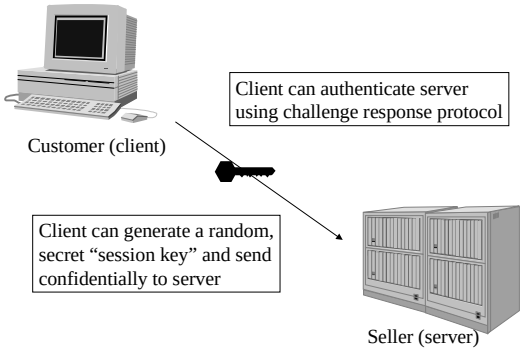


33

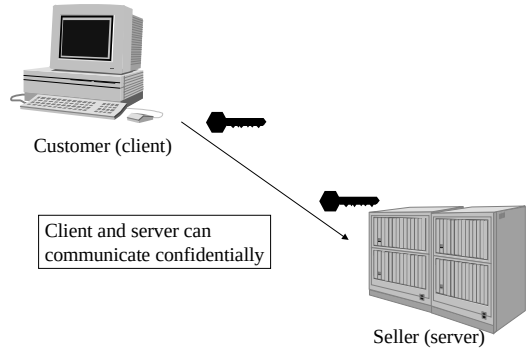
Consumer electronic commerce



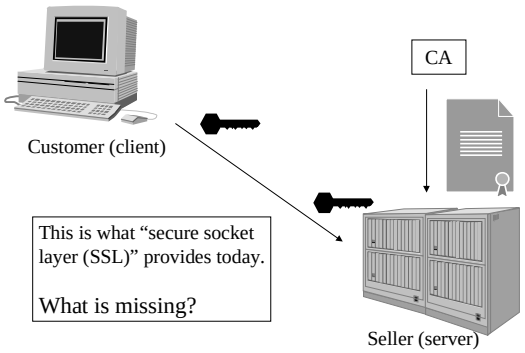
34



35



36



37

Certificate infrastructure

- Certificate authorities
- Individual and corporate certificates
- Benefits:
  - Authentication of sellers and buyers
    - Avoid sales to minors etc.
  - Non-repudiation of transactions

38

Privacy concerns

- On-line transactions can be tracked
- Traditional opposition to "identity card" for this reason
- Safeguards are possible
  - Example: Secure Electronic Transactions (SET)

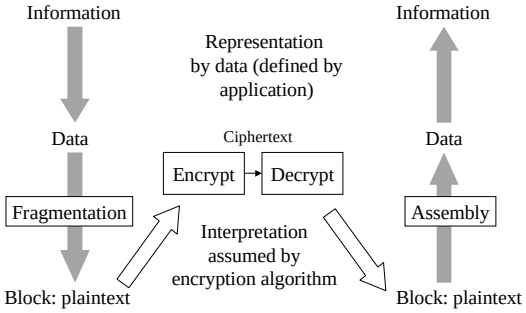
39

Understanding Networked Applications:
A First Course

Slides for Supplements

by
David G. Messerschmitt

Encryption obscures data representation



41

Block substitution table

Plaintext (n bits)	Ciphertext (n bits)
0000000000000	0100001011001
0000000000001	0111010011000
0000000000010	1000101101011
….	….
1111111111111	1110100000110

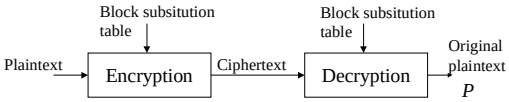
42

Block substitution table

Plaintext (n bits)	Ciphertext (n bits)
For each of the 2^n possible plaintext blocks	The substitute ciphertext block of n bits

The table has $n \cdot 2^n$ bits total

Confidentiality based on the block substitution cipher



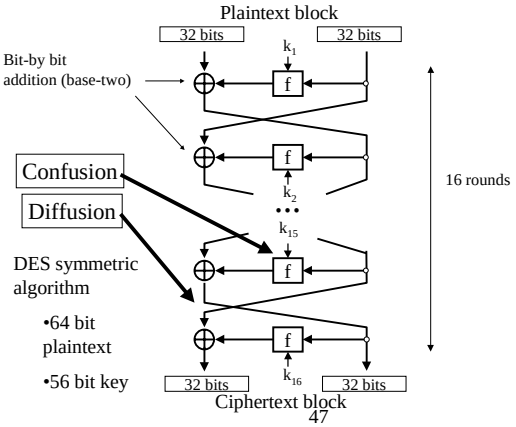
- This is a symmetric encryption/decryption algorithm
- The *key* is the *table*, which has $n \cdot 2^n$ bits

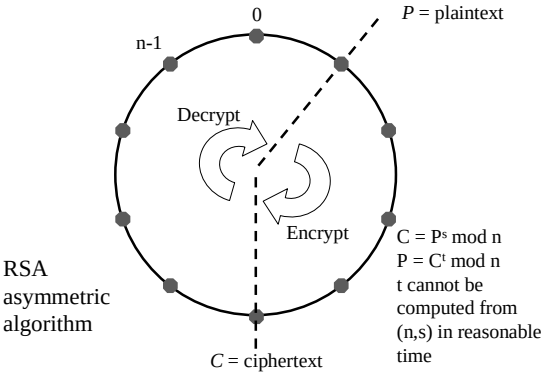
Practicality

- For small block size n, statistical techniques can easily infer the table
- For large block size n, the table is too large to be practical
  - e.g. n=64, $n \cdot 2^n = 10^{21}$, far greater than the total storage in a computer

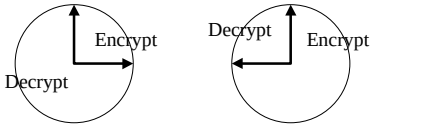
Practicality (con't)

- Keys need not be as large for an exhaustive key trial attack
  - e.g. 10^9 trials/sec, 10 years = 3×10^8 sec
  - 3×10^{17} trials in 10 years
  - $2^{59} = 6 \times 10^{17}$
  - 59 bit key will do it!
- Conclusion: need an encryption algorithm!
  - Key with 64 or 128 bits may be enough





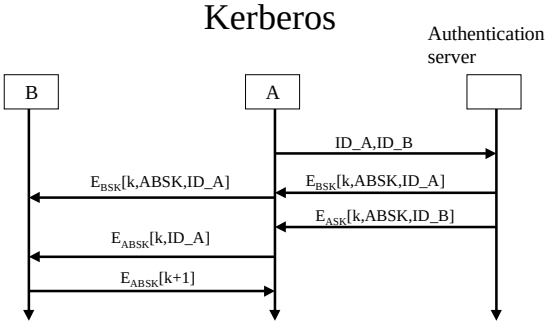
Notice the asymmetry



The two keys can be applied in either order, and we still return to where we started

49

Kerberos



50