Chapter 4

Authentication Applications

Henric Johnson

Blekinge Institute of Technology,Sweden

http://www.its.bth.se/staff/hjo/

henric.johnson@bth.se

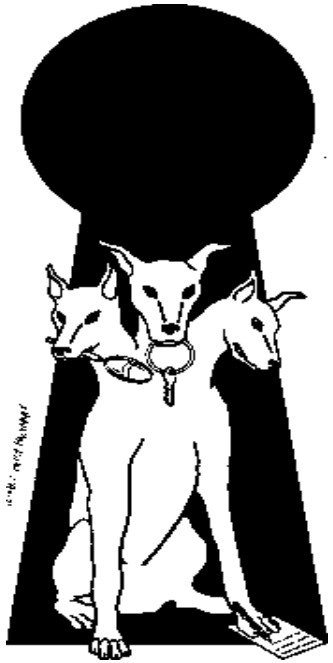
Outline

- Security Concerns
- Kerberos
- X.509 Authentication Service
- Recommended reading and Web Sites

Security Concerns

- key concerns are **confidentiality** and **timeliness**
- to provide confidentiality must encrypt identification and session key info
- which requires the use of previously shared private or public keys
- need timeliness to prevent **replay attacks**
- provided by using sequence numbers or timestamps or challenge/response

KERBEROS



In Greek mythology, a many headed dog, the guardian of the entrance of Hades

KERBEROS

- Users wish to access services on servers.
- Three threats exist:
  - User pretend to be another user.
  - User alter the network address of a workstation.
  - User eavesdrop on exchanges and use a replay attack.

KERBEROS

- Provides a centralized authentication server to authenticate users to servers and servers to users.
- Relies on conventional encryption, making no use of public-key encryption
- Two versions: version 4 and 5
- Version 4 makes use of DES

Kerberos Version 4

- Terms:
  - C = Client
  - AS = authentication server
  - V = server
  - ID_C = identifier of user on C
  - ID_V = identifier of V
  - P_c = password of user on C
  - ADc = network address of C
  - K_V = secret encryption key shared by AS an V
  - TS = timestamp
  - || = concatenation

A Simple Authentication Dialogue

(1) C → AS: $IDc \,||\, P_c \,||\, IDv$

(2) AS → C: Ticket

(3) C → V: $IDc \,||\, Ticket$

$Ticket = E_{Kv}[IDc \,||\, P_c \,||\, IDv]$

Version 4 Authentication Dialogue

- Problems:
  - Lifetime associated with the ticket-granting ticket
  - If too short → repeatedly asked for password
  - If too long → greater opportunity to replay
- The threat is that an opponent will steal the ticket and use it before it expires

Version 4 Authentication Dialogue

Authentication Service Exhange: To obtain Ticket-Granting Ticket

(1) C → AS: IDc || IDtgs ||TS1

(2) AS → C: $E_{Kc}[K_{c,tgs}|| IDtgs || TS_2 || Lifetime_2 || Ticket_{tgs}]$

Ticket-Granting Service Echange: To obtain Service-Granting Ticket

(3) C → TGS: IDv ||$Ticket_{tgs}$ ||Authenticatorc

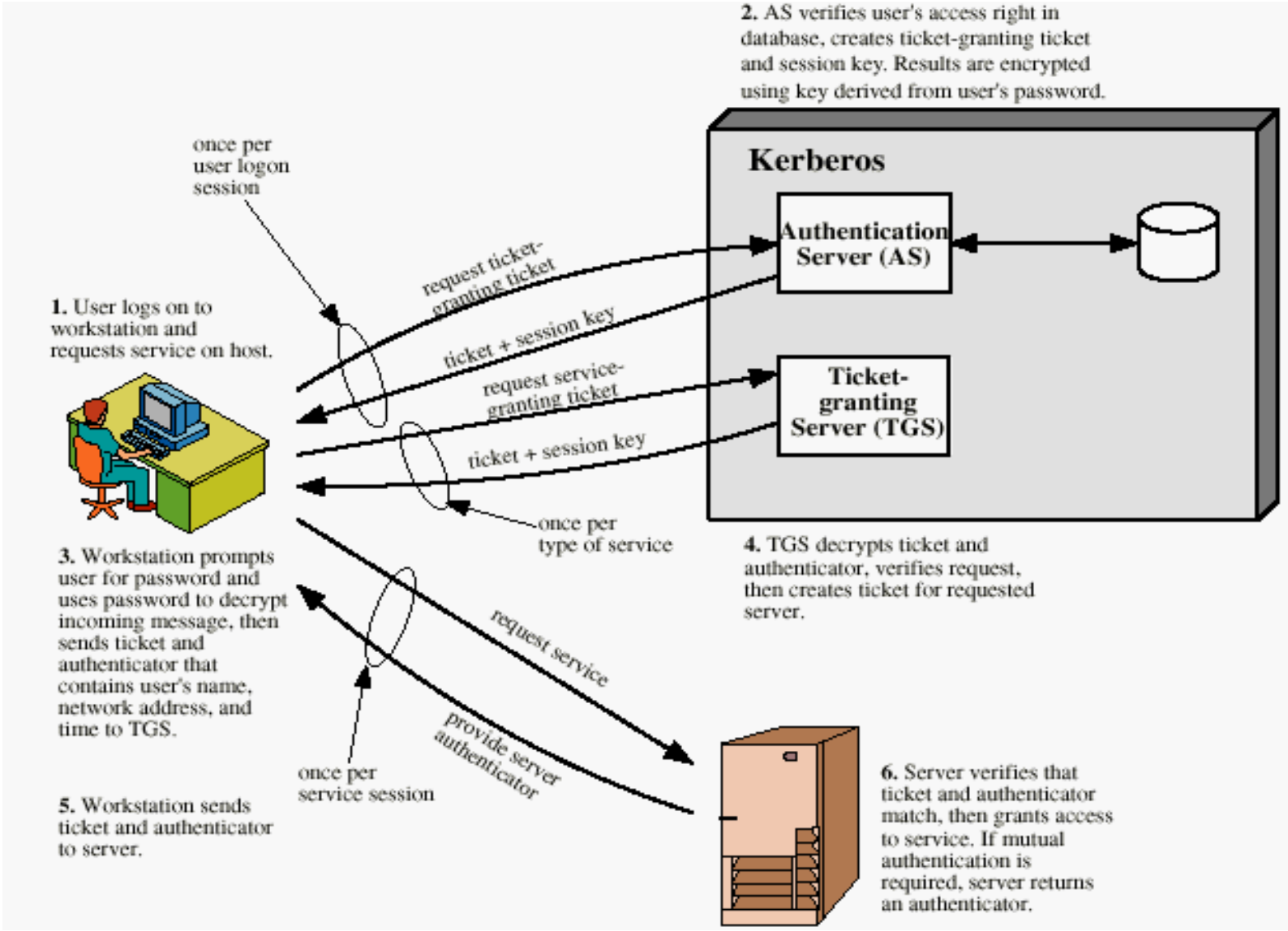
(4) TGS → C: $E_{Kc}[K_{c,v}|| IDv || TS_4 || Ticket_v]$

Client/Server Authentication Exhange: To Obtain Service

(5) C → V: $Ticket_v$ || $Authenticator_c$

(6) V → C: EKc,v[TS5 +1]

Overview of Kerberos



Request for Service in Another Realm

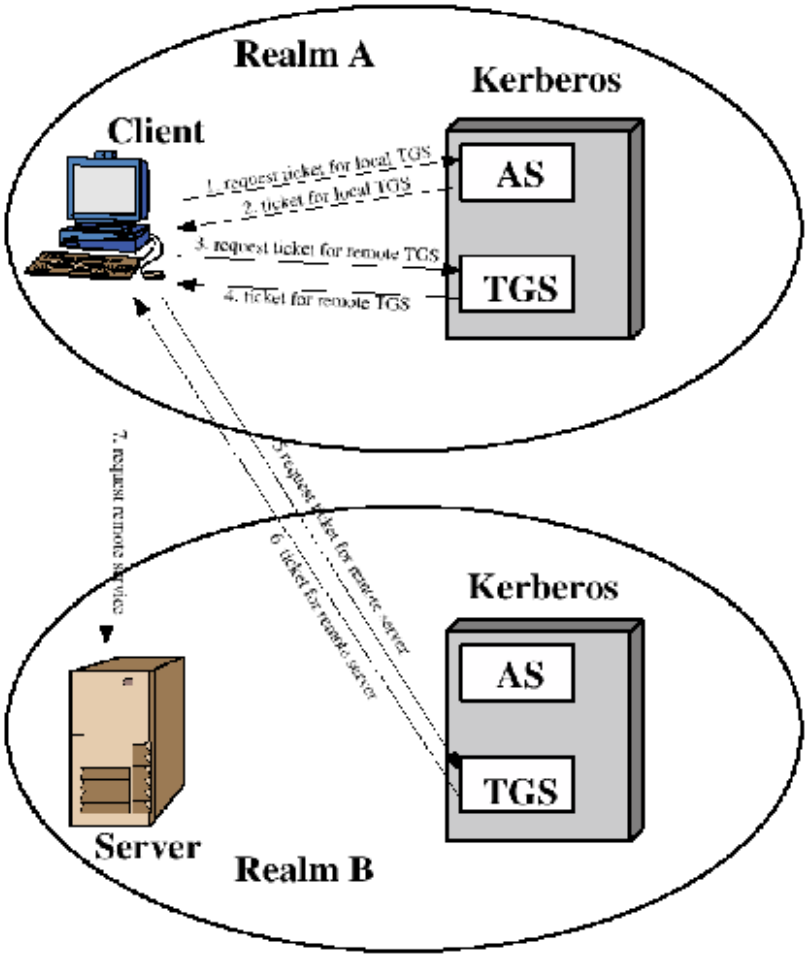


Figure 4.2 Request for Service in Another Realm

Difference Between Version 4 and 5

- Encryption system dependence (V.4 DES)
- Internet protocol dependence
- Message byte ordering
- Ticket lifetime
- Authentication forwarding
- Interrealm authentication

Kerberos Encryption Techniques

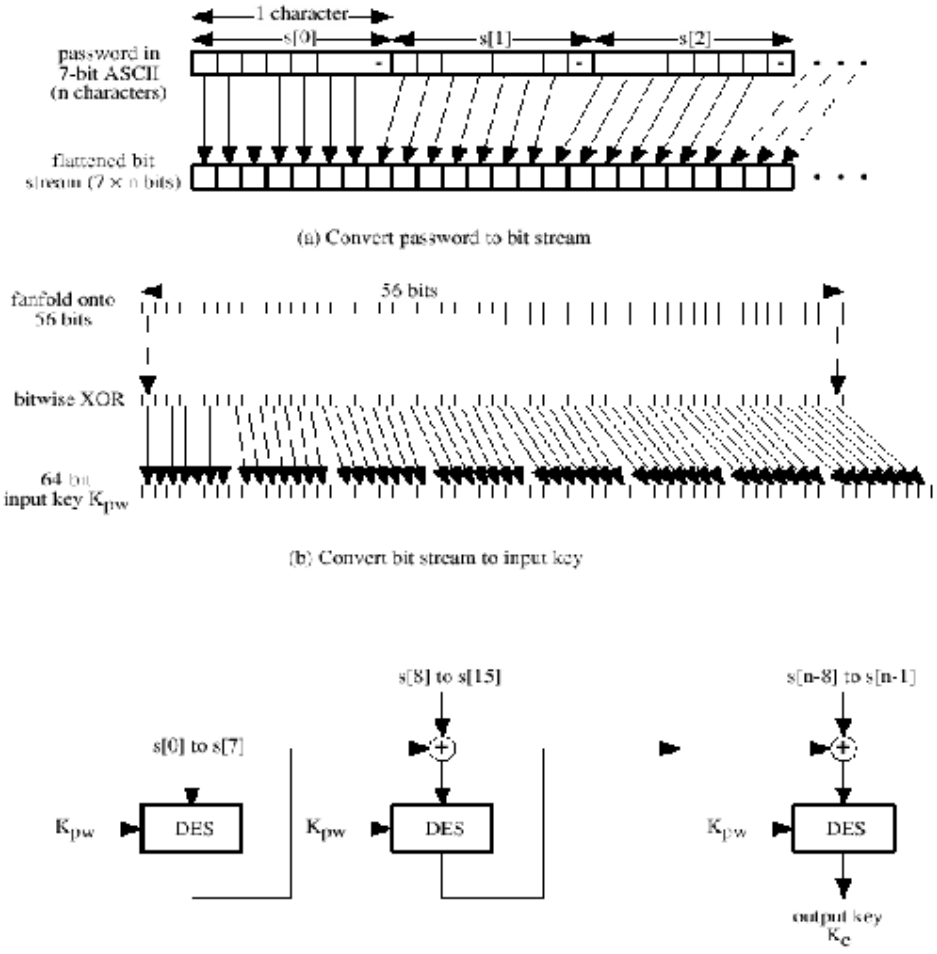


Figure 4.6 Generation of Encryption Key from Password

PCBC Mode

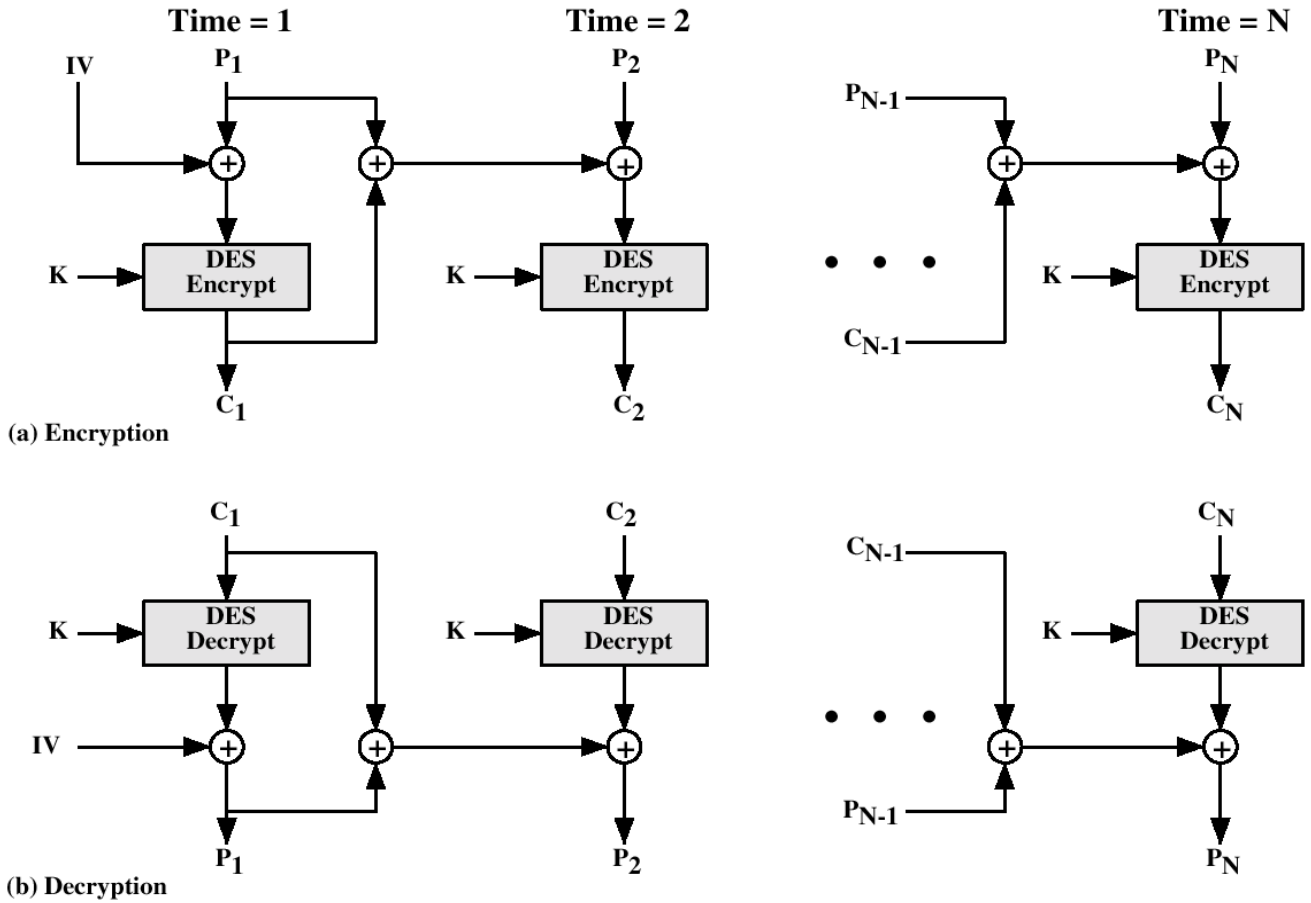


Figure 4.7 Propagating Cipher Block Chaining (PCBC) Mode

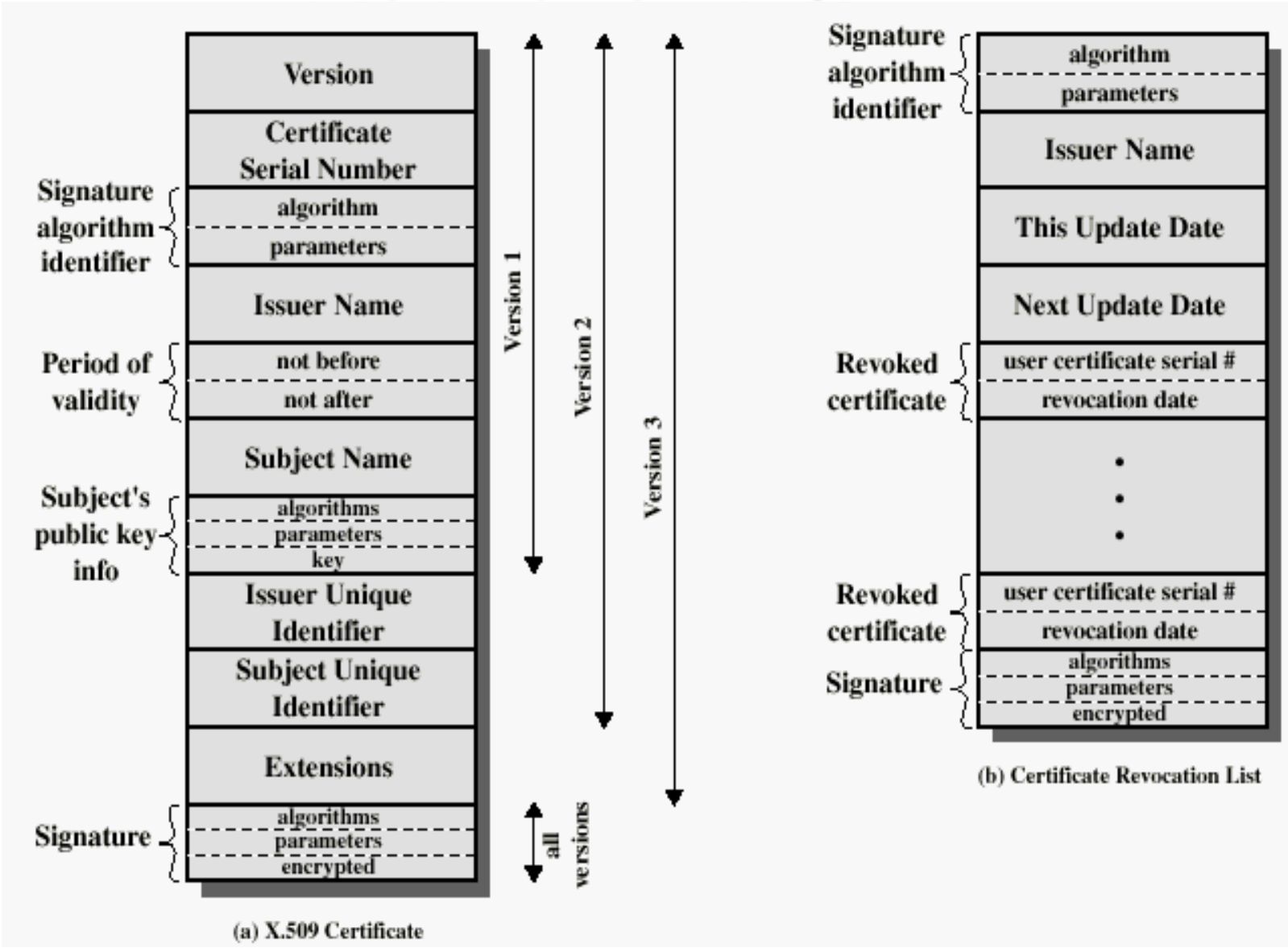
Kerberos - in practice

- **Currently have two Kerberos versions:**
- 4 : restricted to a single realm
- 5 : allows inter-realm authentication, in beta test
- Kerberos v5 is an Internet standard
- specified in RFC1510, and used by many utilities
- **To use Kerberos:**
- need to have a KDC on your network
- need to have Kerberised applications running on all participating systems
- major problem - US export restrictions
- Kerberos cannot be directly distributed outside the US in source format (& binary versions must obscure crypto routine entry points and have no encryption)
- else crypto libraries must be reimplemented locally

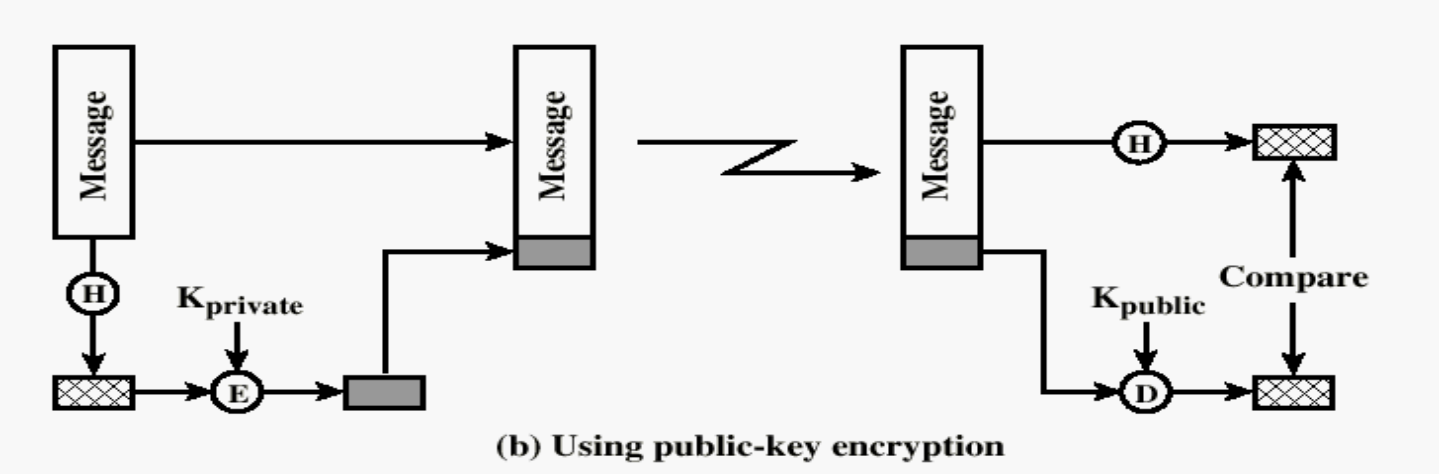
X.509 Authentication Service

- Distributed set of servers that maintains a database about users.
- Each certificate contains the public key of a user and is signed with the private key of a CA.
- Is used in S/MIME, IP Security, SSL/TLS and SET.
- RSA is recommended to use.

X.509 Formats



Typical Digital Signature Approach

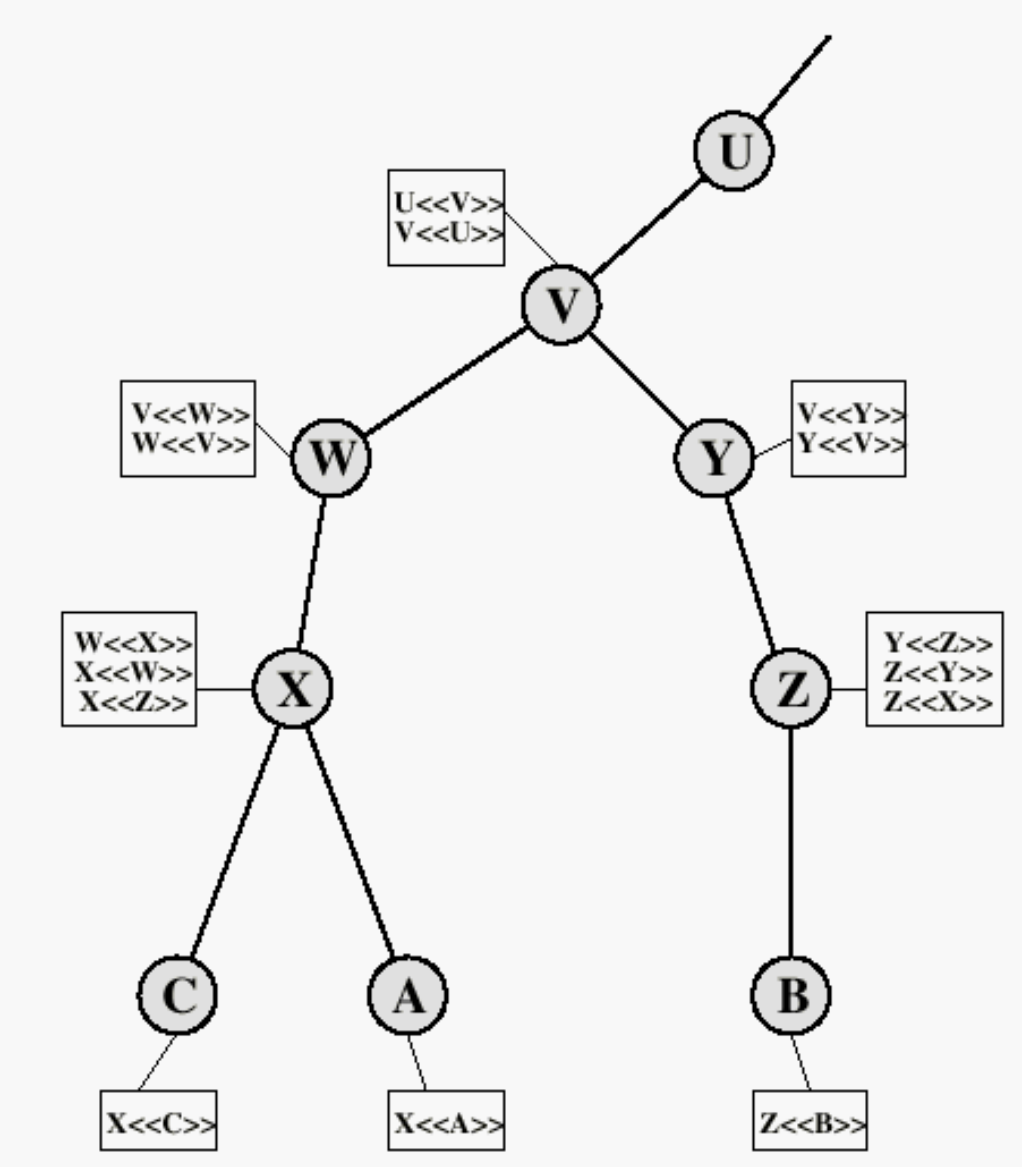


(b) Using public-key encryption

Obtaining a User's Certificate

- Characteristics of certificates generated by *CA*:
  - Any user with access to the public key of the *CA* can recover the user public key that was certified.
  - No part other than the *CA* can modify the certificate without this being detected.

X.509 CA Hierarchy



Revocation of Certificates

- Reasons for revocation:
  - The users secret key is assumed to be compromised.
  - The user is no longer certified by this CA.
  - The CA's certificate is assumed to be compromised.

Authentication Procedures

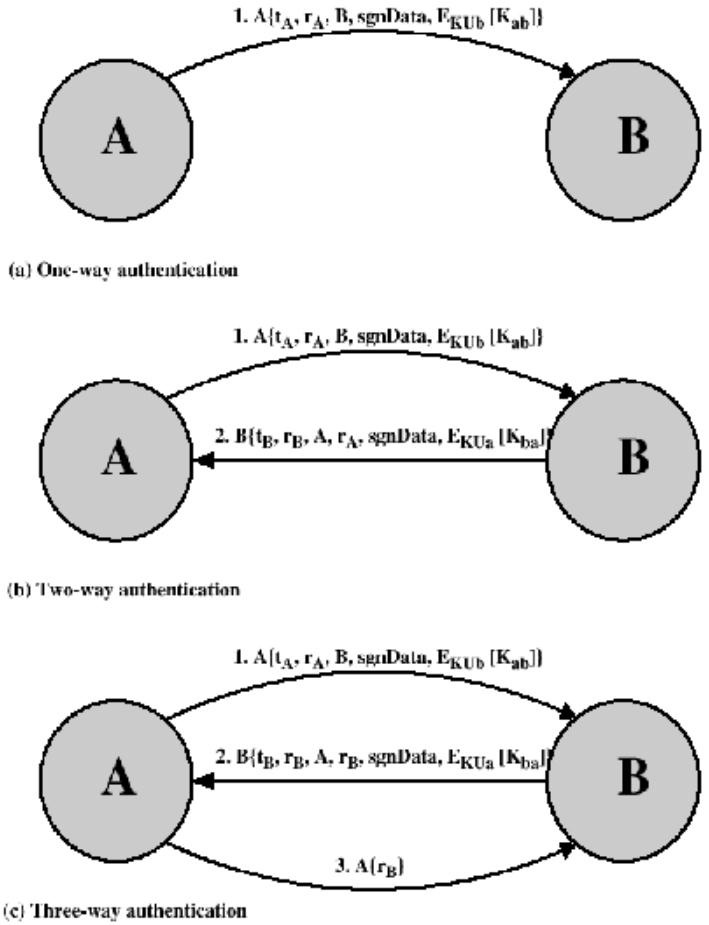


Figure 4.5 X.509 Strong Authentication Procedures

Recommended Reading and WEB Sites

- www.whatis.com (search for kerberos)
- Bryant, W. Designing an Authentication System: A Dialogue in Four Scenes. http://web.mit.edu/kerberos/www/dialogue.html
- Kohl, J.; Neuman, B. "The Evolotion of the Kerberos Authentication Service" http://web.mit.edu/kerberos/www/papers.html
- http://www.isi.edu/gost/info/kerberos/