Security

Chapter 8

Types of Threats

- Interception, Perangkat sistem menjadi rusak atau tidak tersedia.Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah “denial of service attack”.
- Interruption, Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).
- Modification, Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan pesan yang merugikan pemilik web site.
- Fabrication, Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

Security Policy

Menggambarkan Aksi yang tepat untuk entiti pada sebuah sistem yang dibolehkan (“allow”) atau dilarang (“Prohibited”)

Security Mechanisms

- Encryption
- Authentication
- Authorization
- Auditing

Encryption

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak.

1. Dengan enkripsi data anda disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*).
2. Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (untuk kasus *private keycryptography*) atau dengan kunci yang berbeda (untuk kasus *public key cryptography*)

Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul betul server yang asli.

Masalah yang Muncul :

1. Masalah pertama, membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermarking* dan digital signature.
2. Masalah kedua biasanya berhubungan dengan access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi.

Authorization

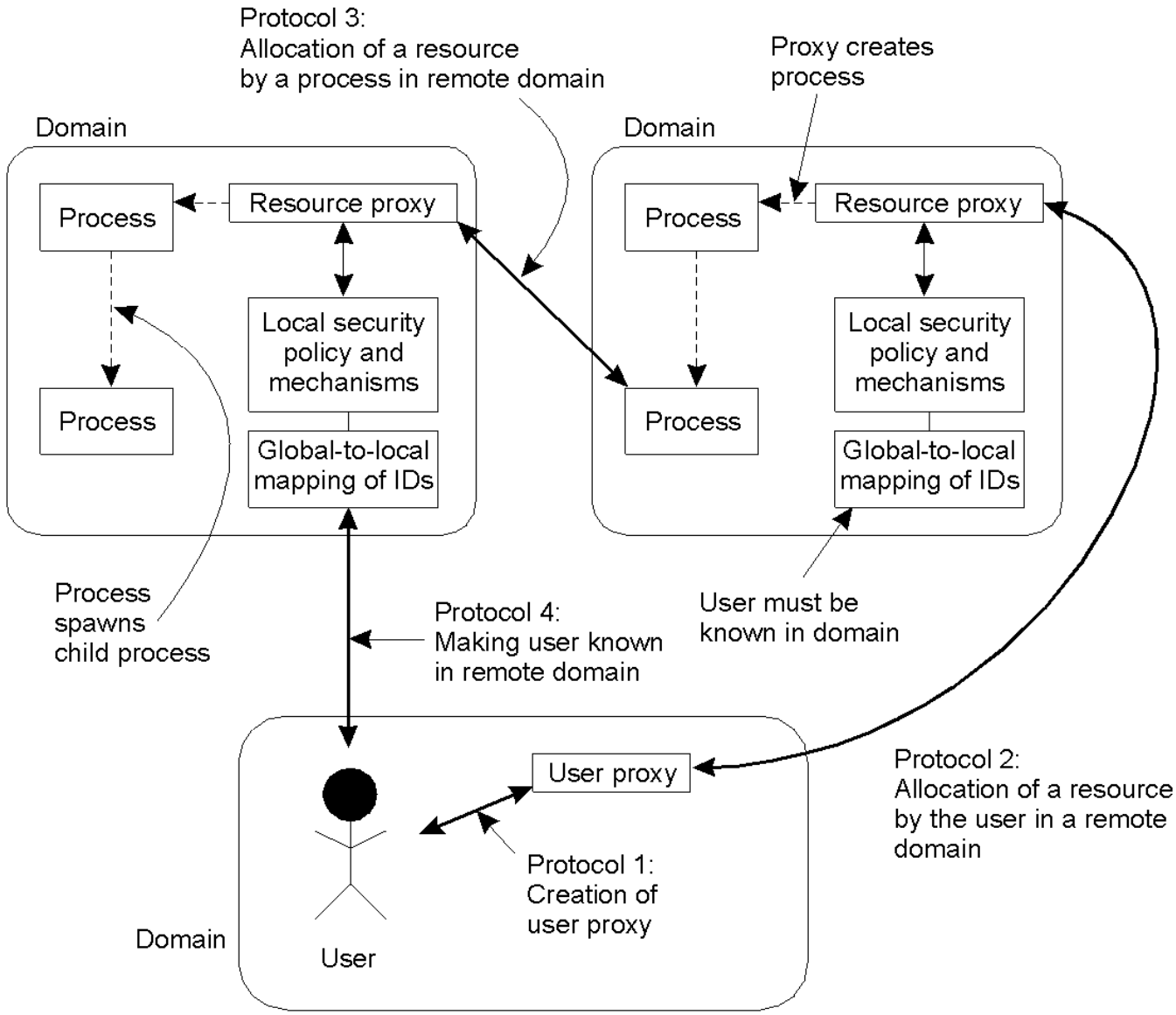
Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (public, private, confidential, top secret) & user (guest, admin, top manager, dsb.), mekanisme authentication dan juga privacy. Access control seringkali dilakukan dengan menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain (seperti kartu, biometrics).

Auditing

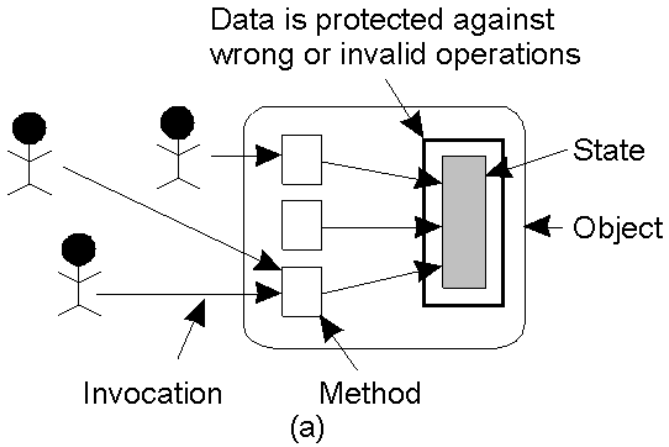
Segala (sebagian besar) kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasanya disebut "*logfile*" atau "*log*" saja. Berkas log ini sangat berguna untuk mengamati penyimpangan yang terjadi. Kegagalan untuk masuk ke sistem (login), misalnya, tersimpan di dalam berkas log. Untuk itu para administrator diwajibkan untuk rajin memelihara dan menganalisa berkas log yang dimilikinya.

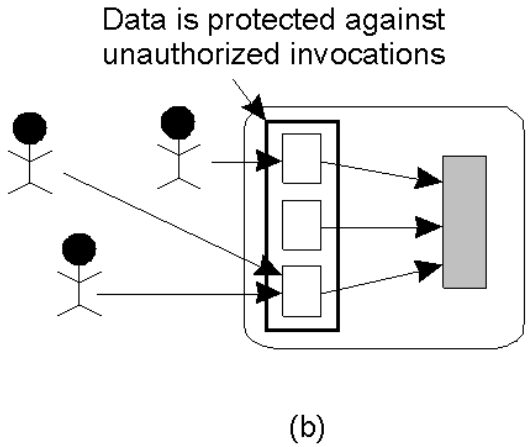
Example: Globus Security Architecture

Diagram of Globus security architecture.



Focus of Control



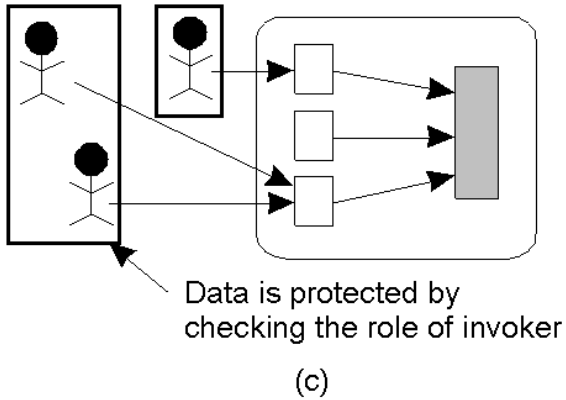


Three approaches for protection against security threats

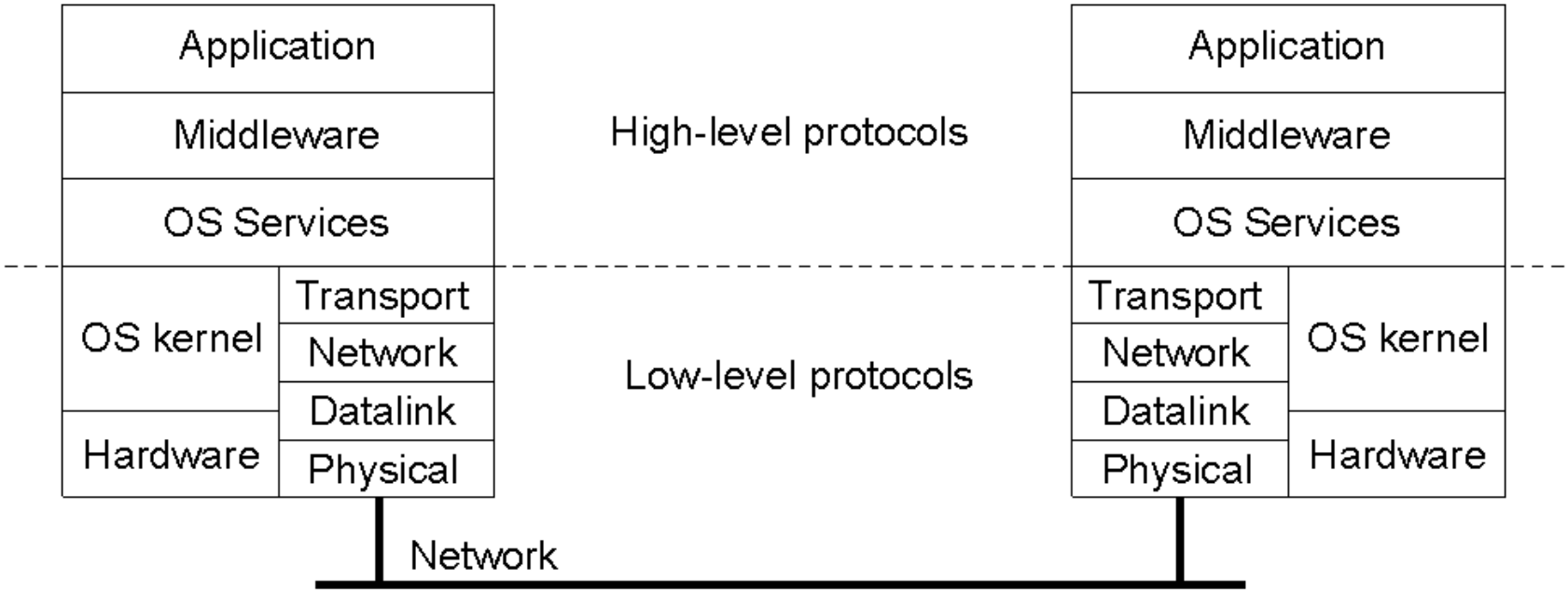
a) Protection against invalid operations

b) Protection against unauthorized invocations

c) Protection against unauthorized users

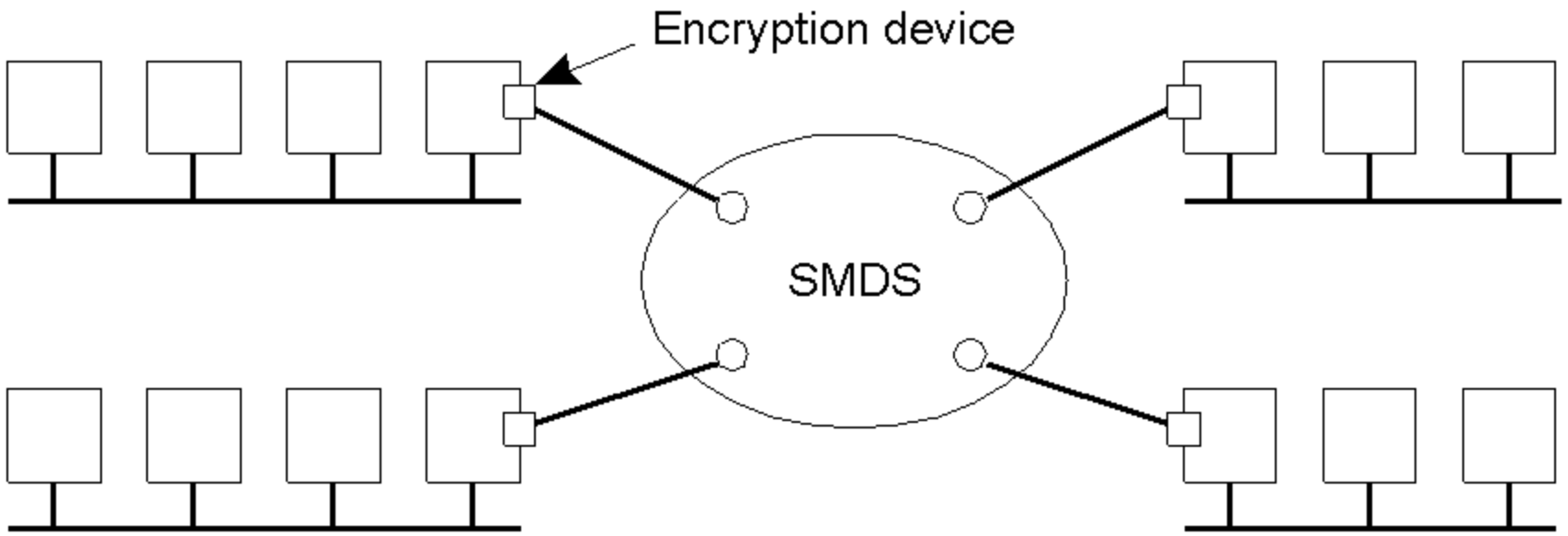


Layering of Security Mechanisms (1)



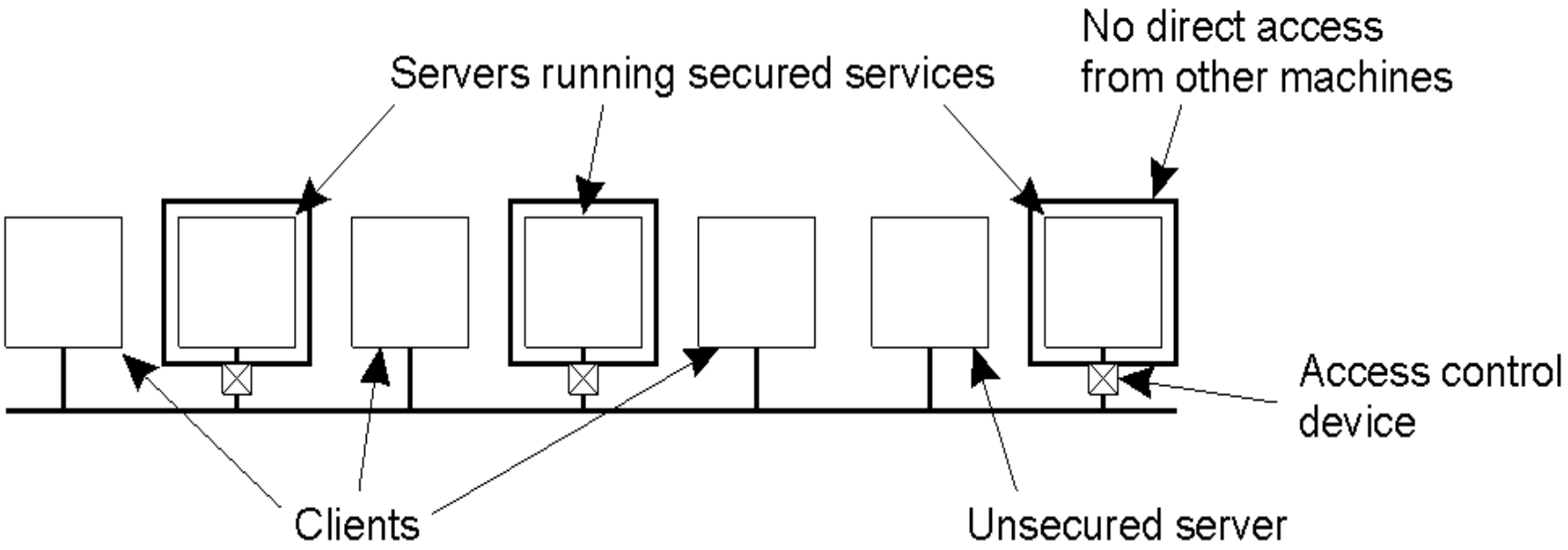
The logical organization of a distributed system into several layers.

Layering of Security Mechanisms (2)



Several sites connected through a wide-area backbone service.

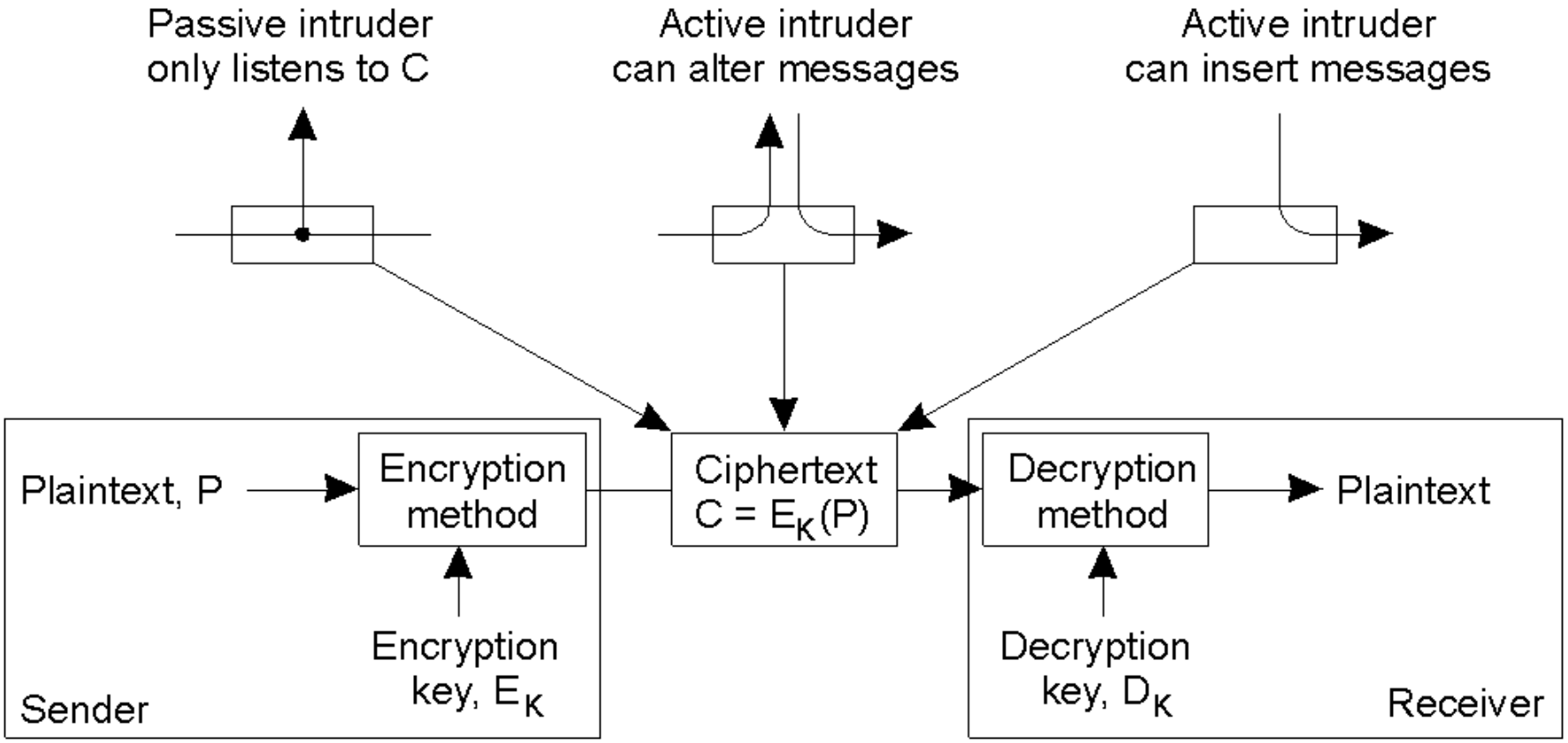
Distribution of Security Mechanisms



The principle of RISSC as applied to secure distributed systems, any security-critical server is placed on separate machine isolated from end-user system using low-level secure network interface

Reduced Interfaces for Secure System Component (RISSC)

Cryptography (1)



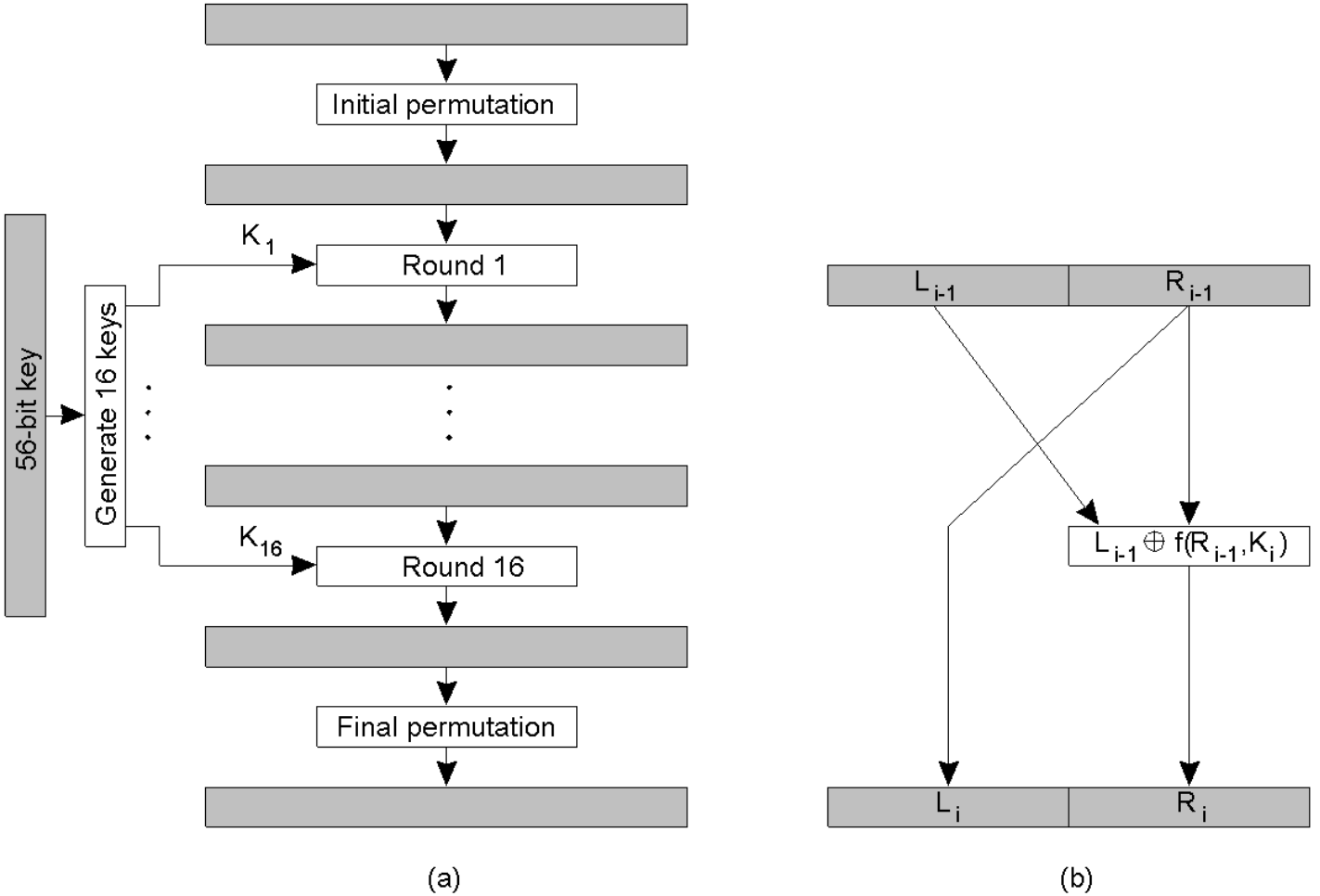
Intruders and eavesdroppers in communication.

Cryptography (2)

Notation	Description
$K_{A, B}$	Secret key shared by A and B
K_A^+	Public key of A
K_A^-	Private key of A

Notation used in this chapter.

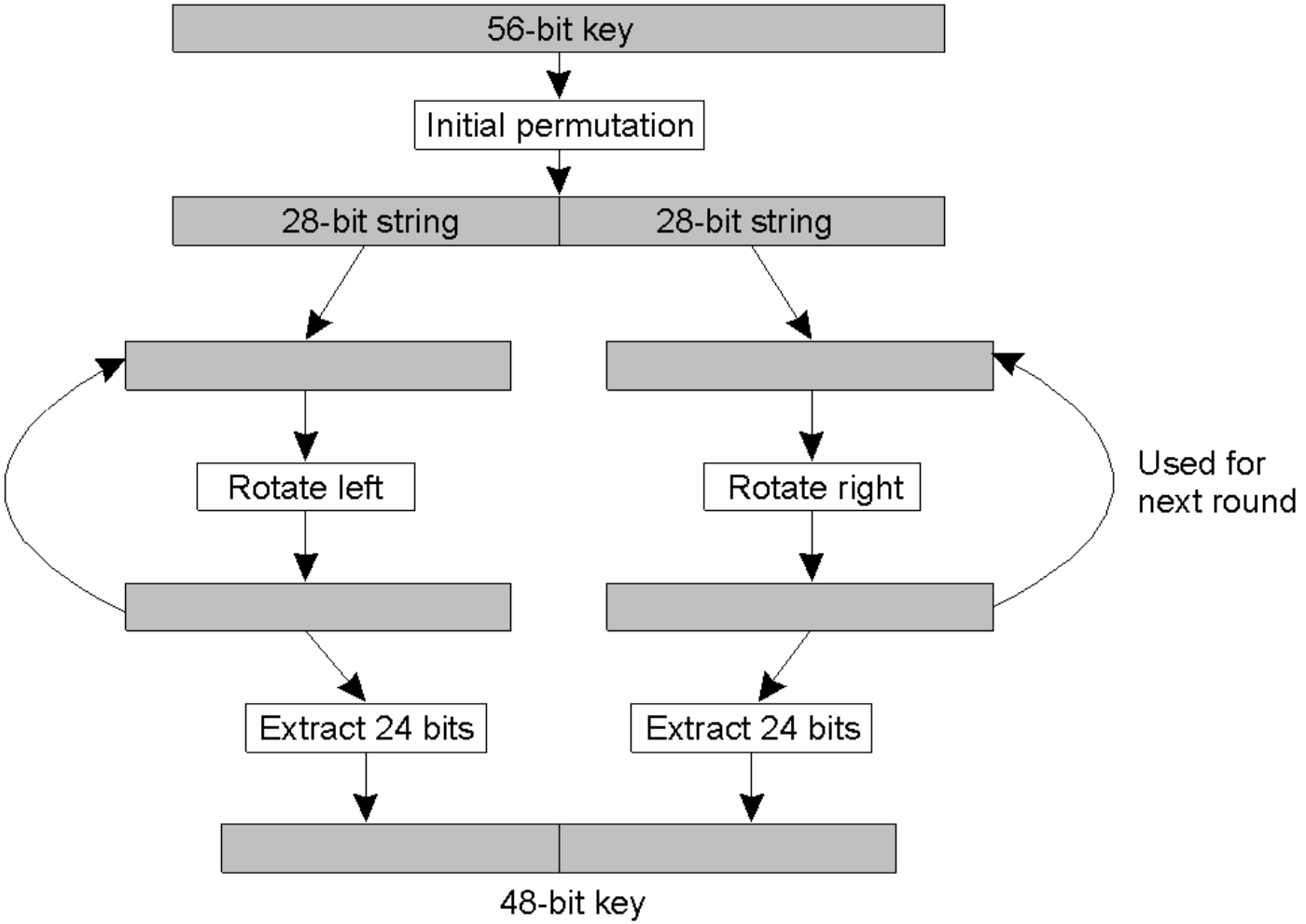
Symmetric Cryptosystems: DES (1)



a) The principle of DES

b) Outline of one encryption round

Symmetric Cryptosystems: DES (2)



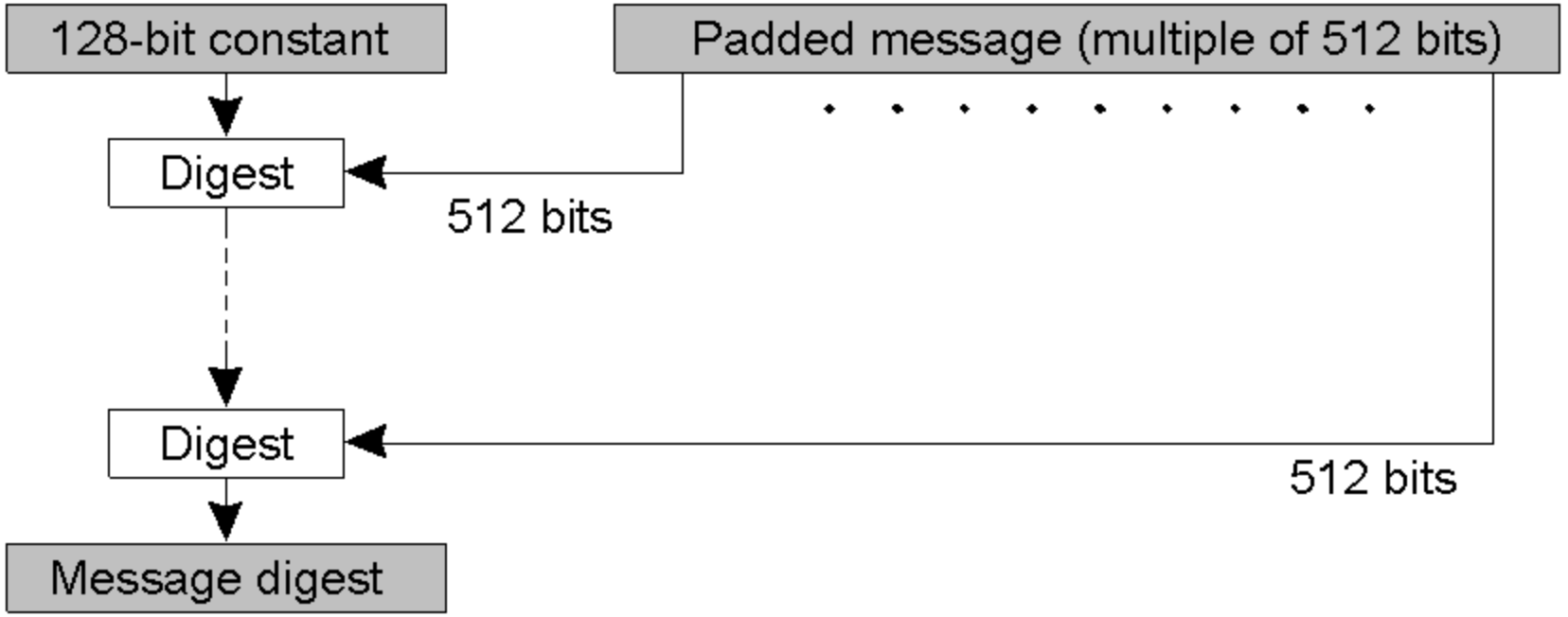
Details of per-round key generation in DES.

Public-Key Cryptosystems: RSA

Generating the private and public key requires four steps:

1. Choose two very large prime numbers, p and q
2. Compute $n = p \times q$ and $z = (p - 1) \times (q - 1)$
3. Choose a number d that is relatively prime to z
4. Compute the number e such that $e \times d = 1 \bmod z$

Hash Functions : MD5 (1)



The structure of MD5

Hash Functions : MD5 (2)

4 Fungsi Pada Setiap Round

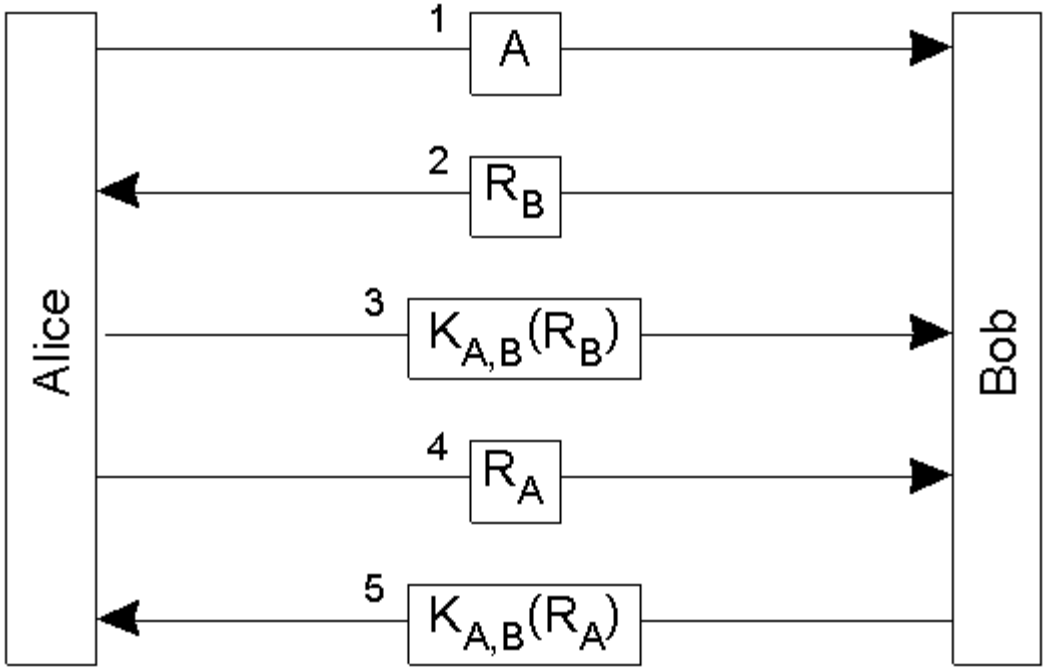
1. F(x,y,z) = (x AND y) OR ((NOT x) AND z)
2. G(x,y,z) = (x AND z) OR (y AND (NOT z))
3. H(x,y,z) = x OR y XOR z
4. I(x,y,z) = y XOR (x OR (NOT z))

Hash Functions : MD5 (3)

Iterations 1-8	Iterations 9-16
$p \leftarrow (p + F(q,r,s) + b_0 + C_1) \lll 7$	$p \leftarrow (p + F(q,r,s) + b_8 + C_9) \lll 7$
$s \leftarrow (s + F(p,q,r) + b_1 + C_2) \lll 12$	$s \leftarrow (s + F(p,q,r) + b_9 + C_{10}) \lll 12$
$r \leftarrow (r + F(s,p,q) + b_2 + C_3) \lll 17$	$r \leftarrow (r + F(s,p,q) + b_{10} + C_{11}) \lll 17$
$q \leftarrow (q + F(r,s,p) + b_3 + C_4) \lll 22$	$q \leftarrow (q + F(r,s,p) + b_{11} + C_{12}) \lll 22$
$p \leftarrow (p + F(q,r,s) + b_4 + C_5) \lll 7$	$p \leftarrow (p + F(q,r,s) + b_{12} + C_{13}) \lll 7$
$s \leftarrow (s + F(p,q,r) + b_5 + C_6) \lll 12$	$s \leftarrow (s + F(p,q,r) + b_{13} + C_{14}) \lll 12$
$r \leftarrow (r + F(s,p,q) + b_6 + C_7) \lll 17$	$r \leftarrow (r + F(s,p,q) + b_{14} + C_{15}) \lll 17$
$q \leftarrow (q + F(r,s,p) + b_7 + C_8) \lll 22$	$q \leftarrow (q + F(r,s,p) + b_{15} + C_{16}) \lll 22$

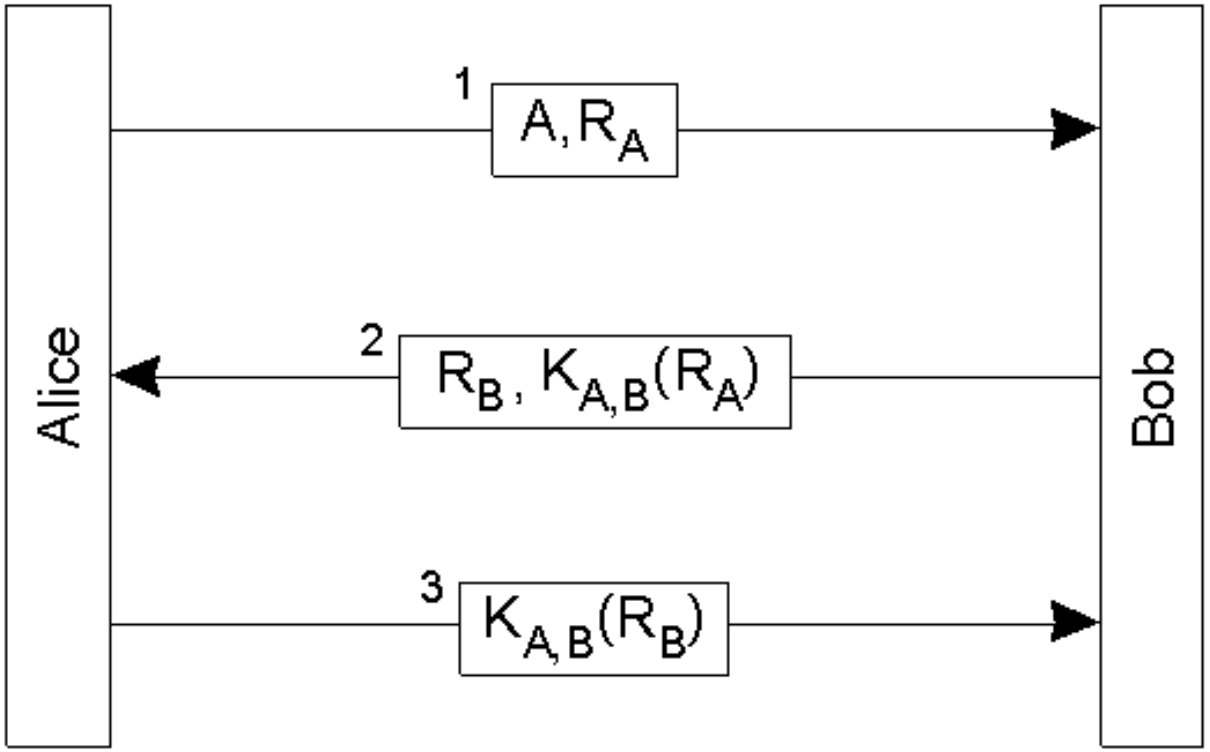
The 16 iterations during the first round in a phase in MD5.

SECURE CHANNEL
Authentication (1)



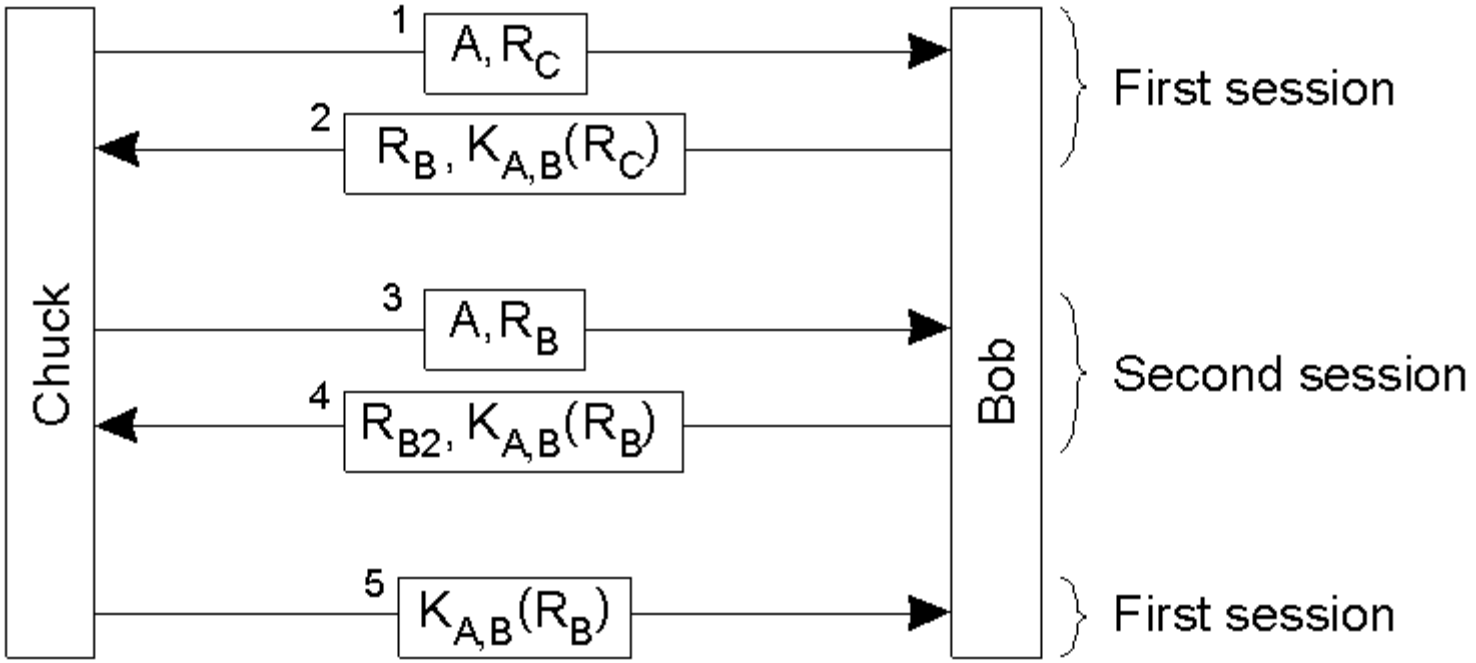
Authentication based on a shared secret key.

Authentication (2)



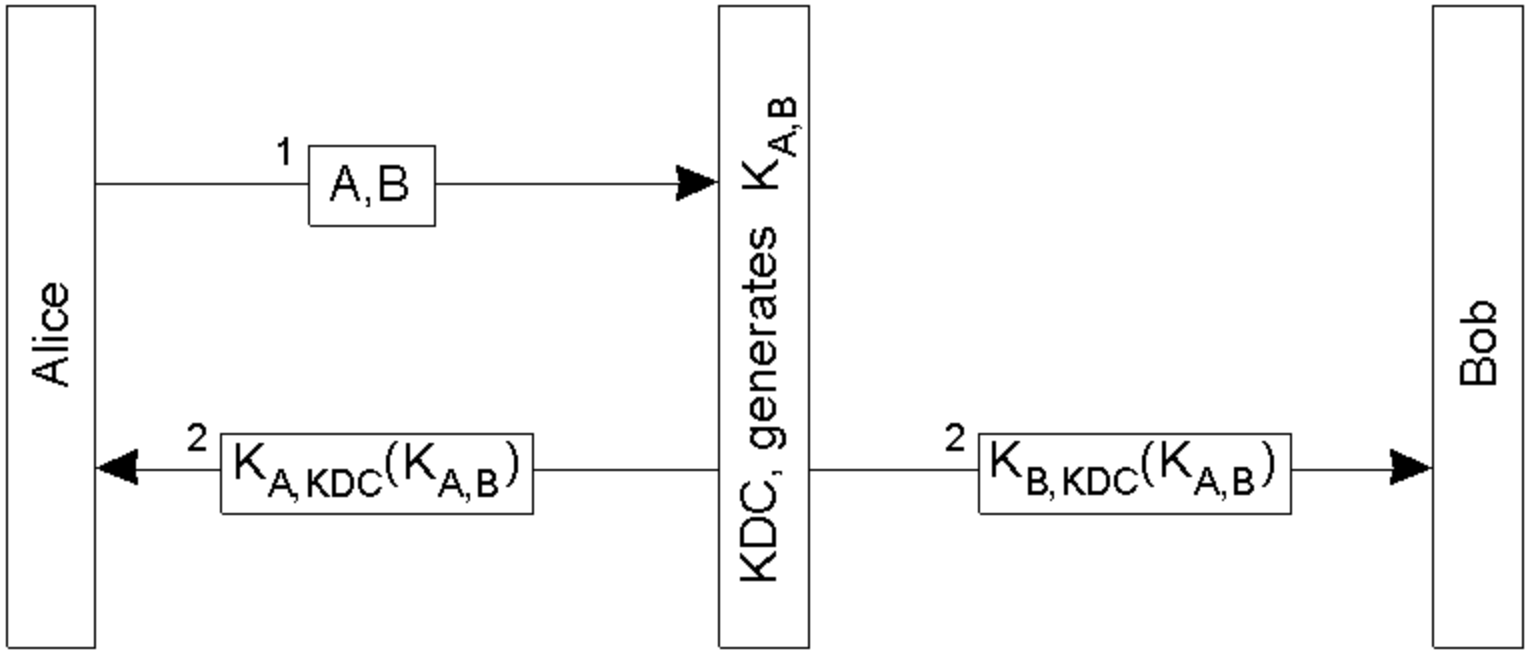
Authentication based on a shared secret key, but using three instead of five messages.

Authentication (3)



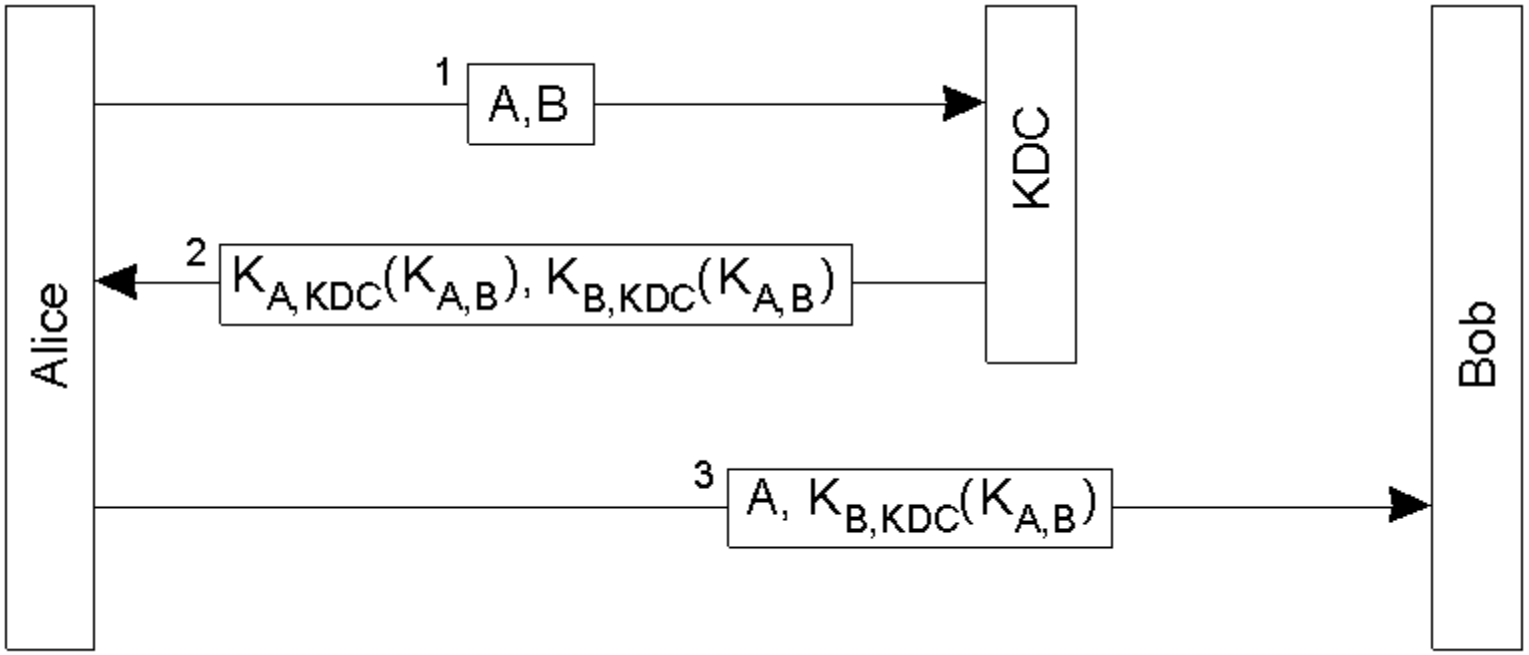
The reflection attack.

Authentication Using a Key Distribution Center (1)



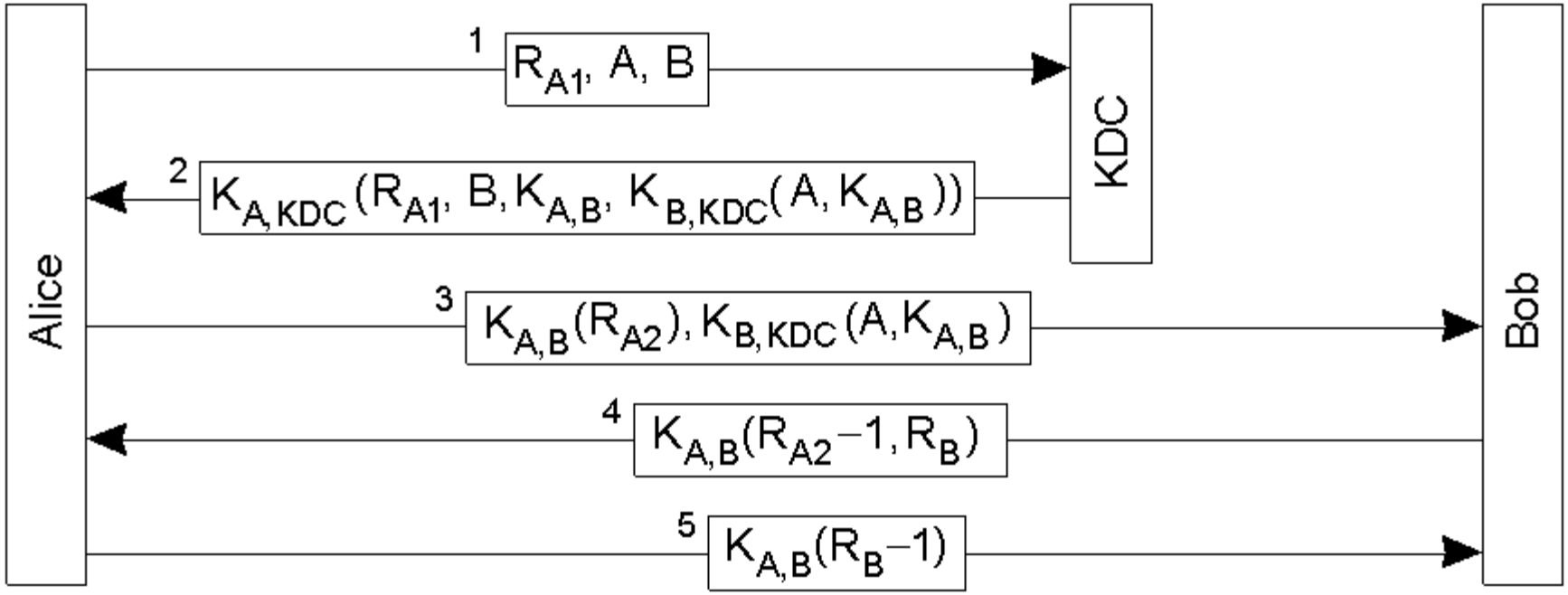
The principle of using a KDC.

Authentication Using a Key Distribution Center (2)



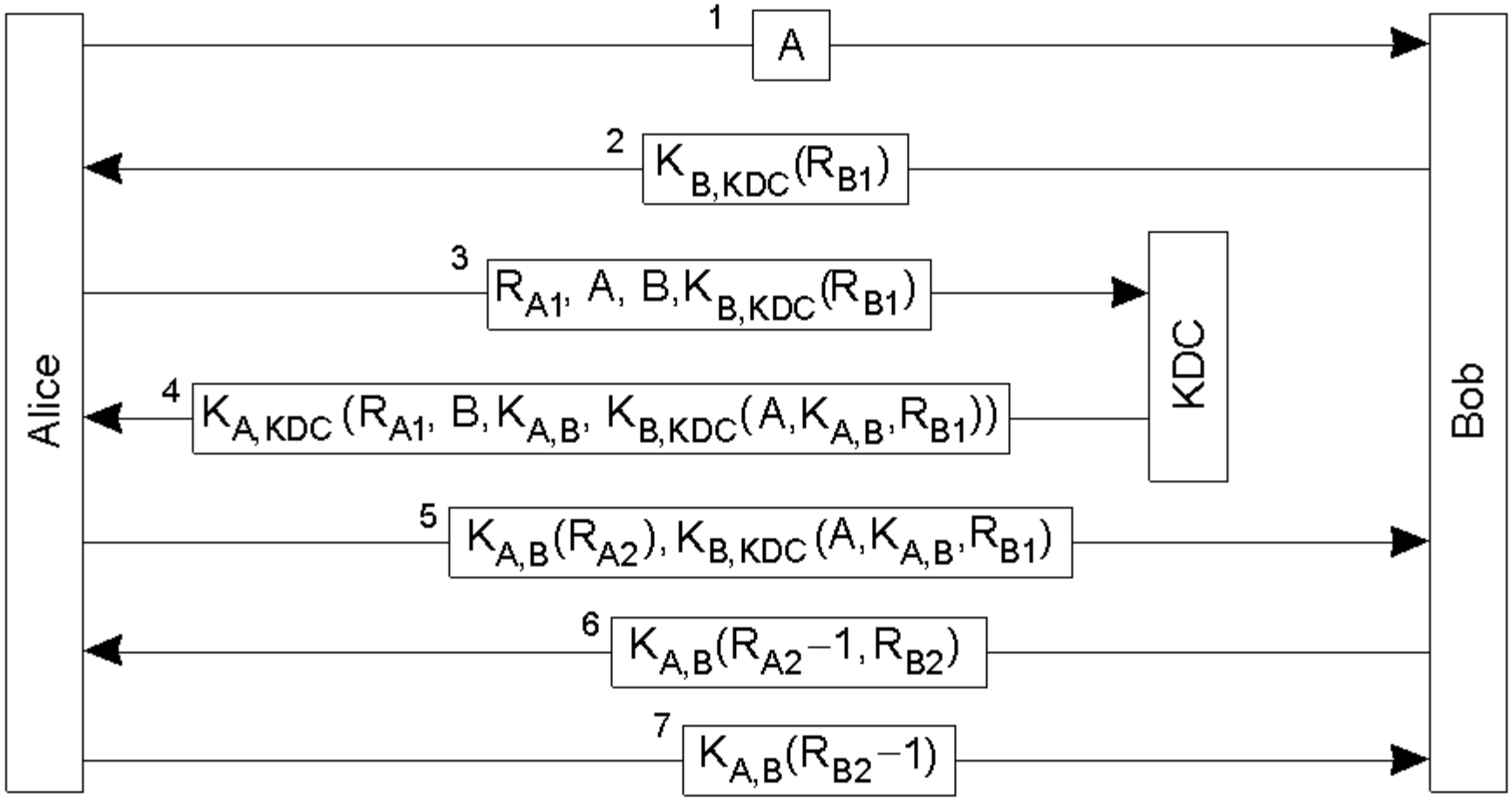
Using a ticket and letting Alice set up a connection to Bob.

Authentication Using a Key Distribution Center (3)



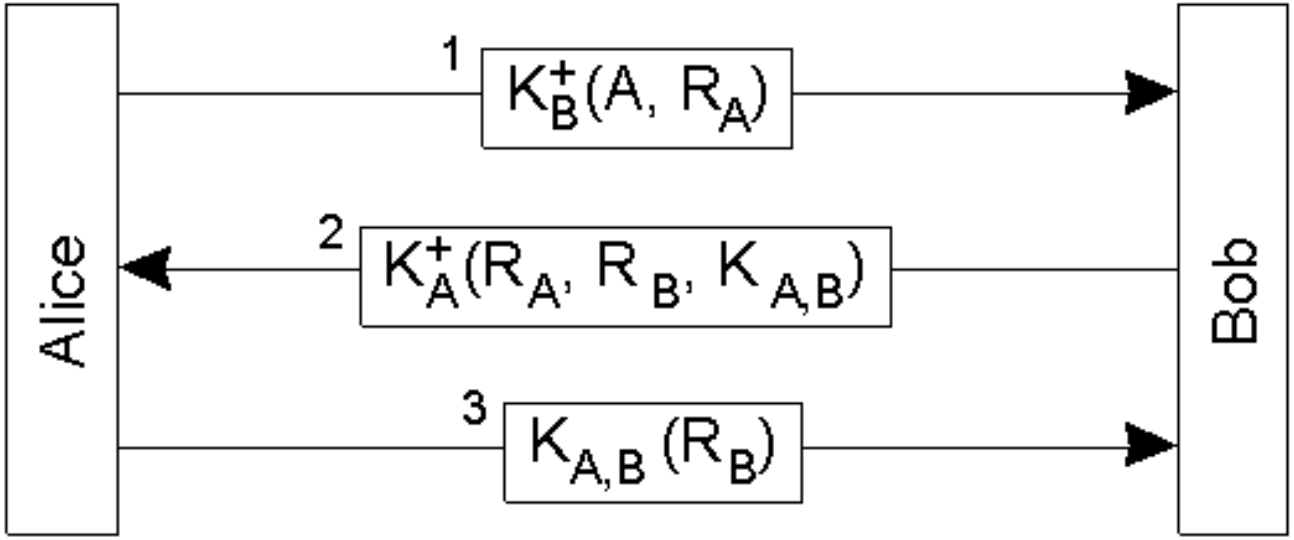
The Needham-Schroeder authentication protocol.

Authentication Using a Key Distribution Center (4)



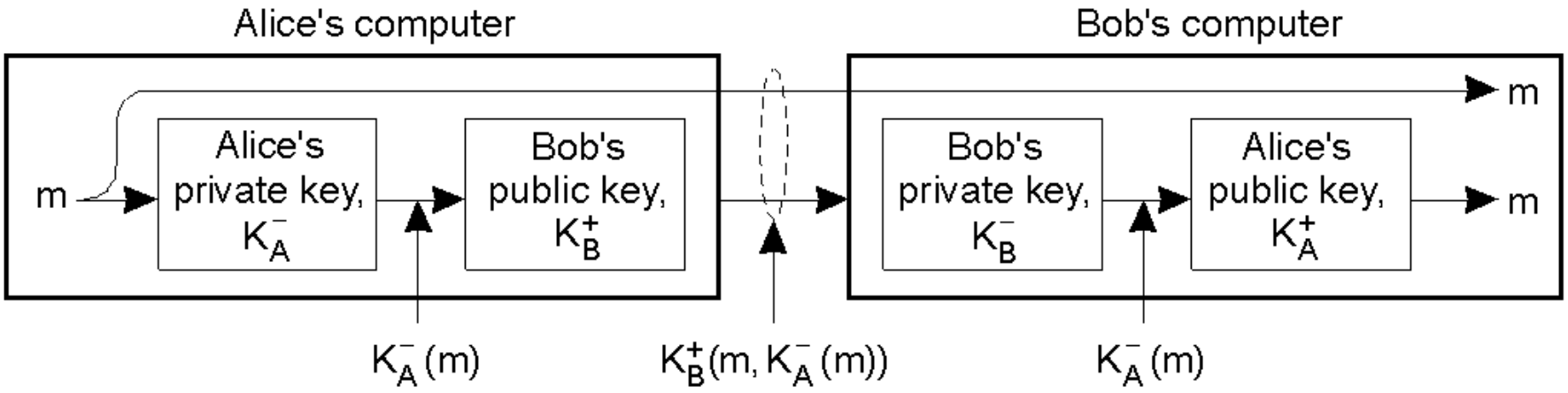
Protection against malicious reuse of a previously generated session key in the Needham-Schroeder protocol.

Authentication Using Public-Key Cryptography



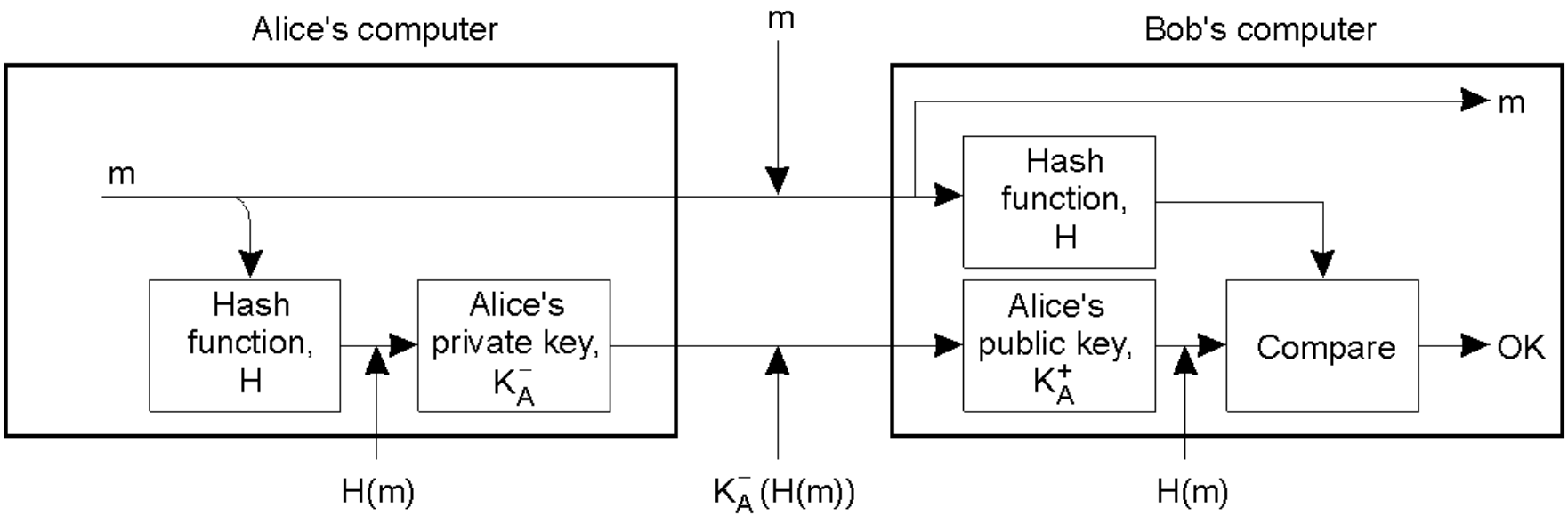
Mutual authentication in a public-key cryptosystem.

Digital Signatures (1)



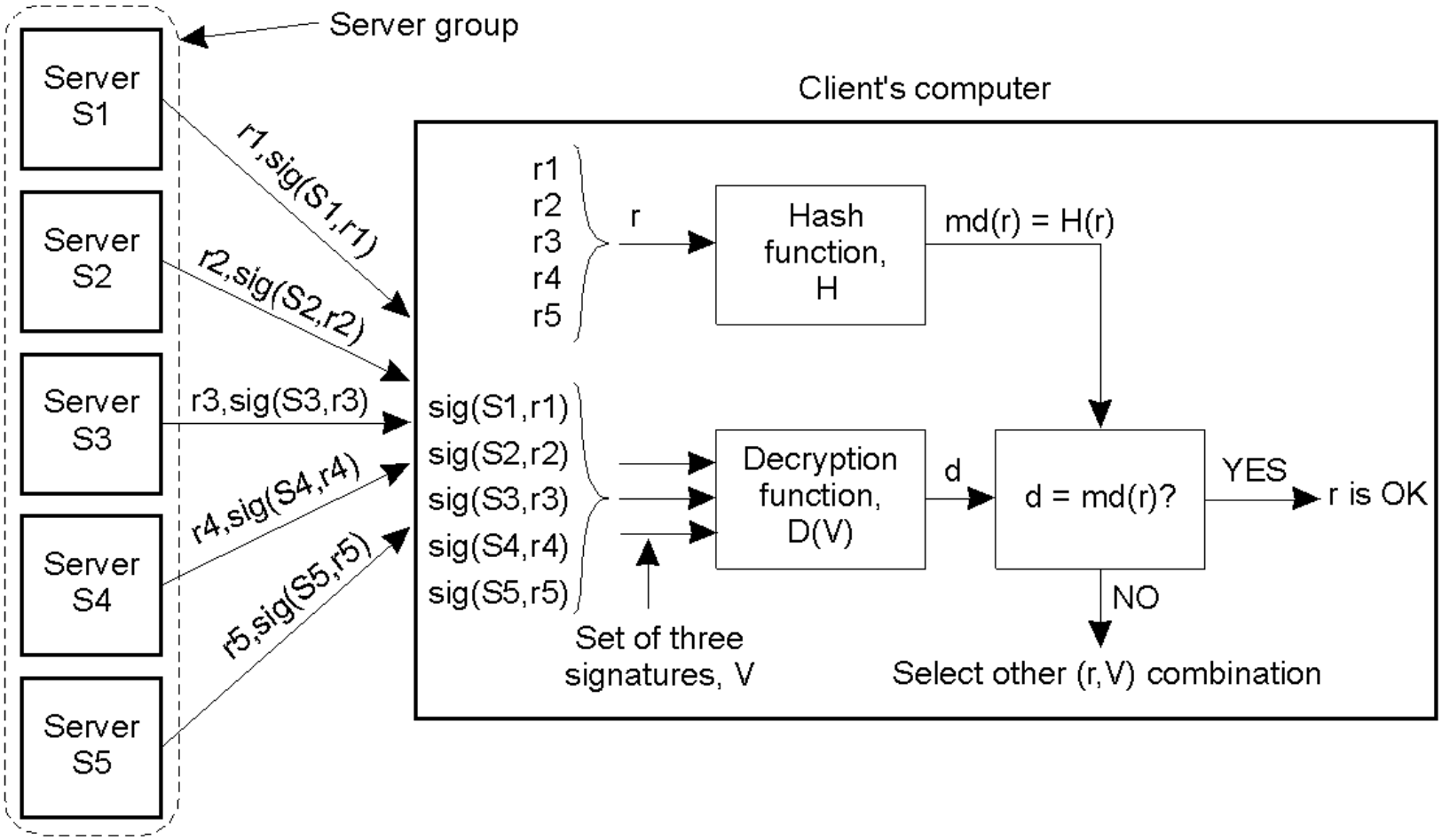
Digital signing a message using public-key cryptography.

Digital Signatures (2)



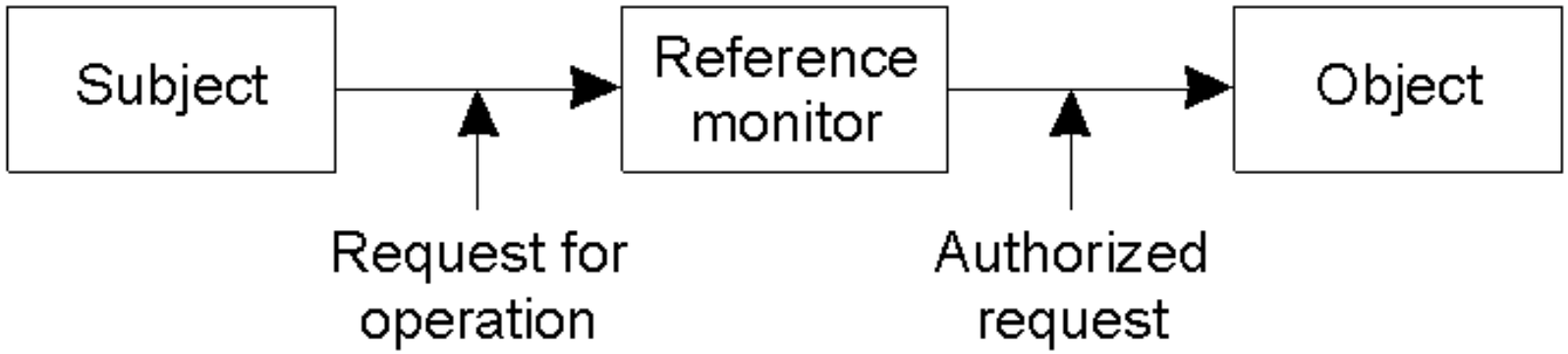
Digitally signing a message using a message digest.

Secure Replicated Services



Sharing a secret signature in a group of replicated servers.

ACCESS CONTROL
General Issues in Access Control



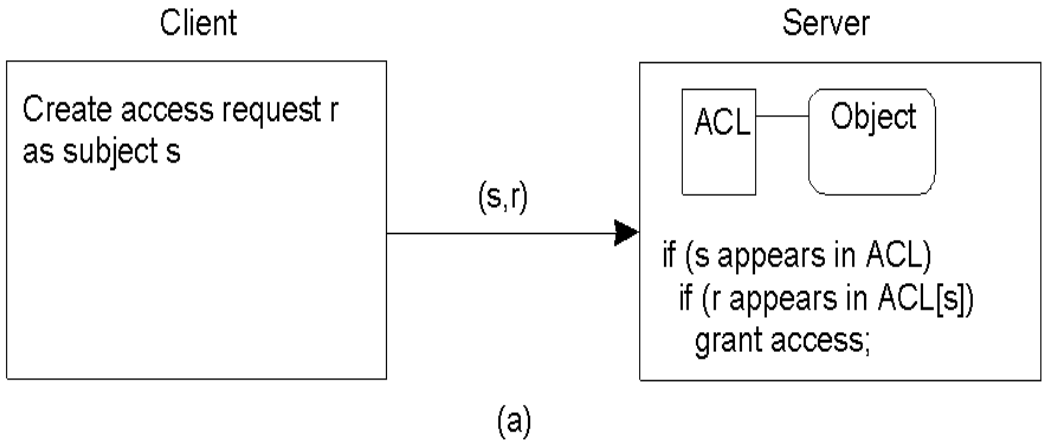
General model of controlling access to objects.

Access Control Matrix

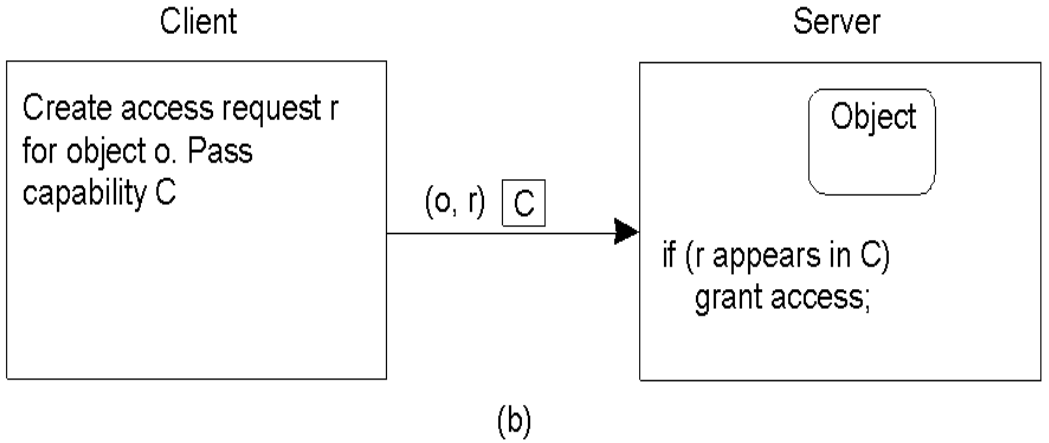
Comparison between ACLs and capabilities for protecting objects.

a) Using an ACL

b) Using capabilities.

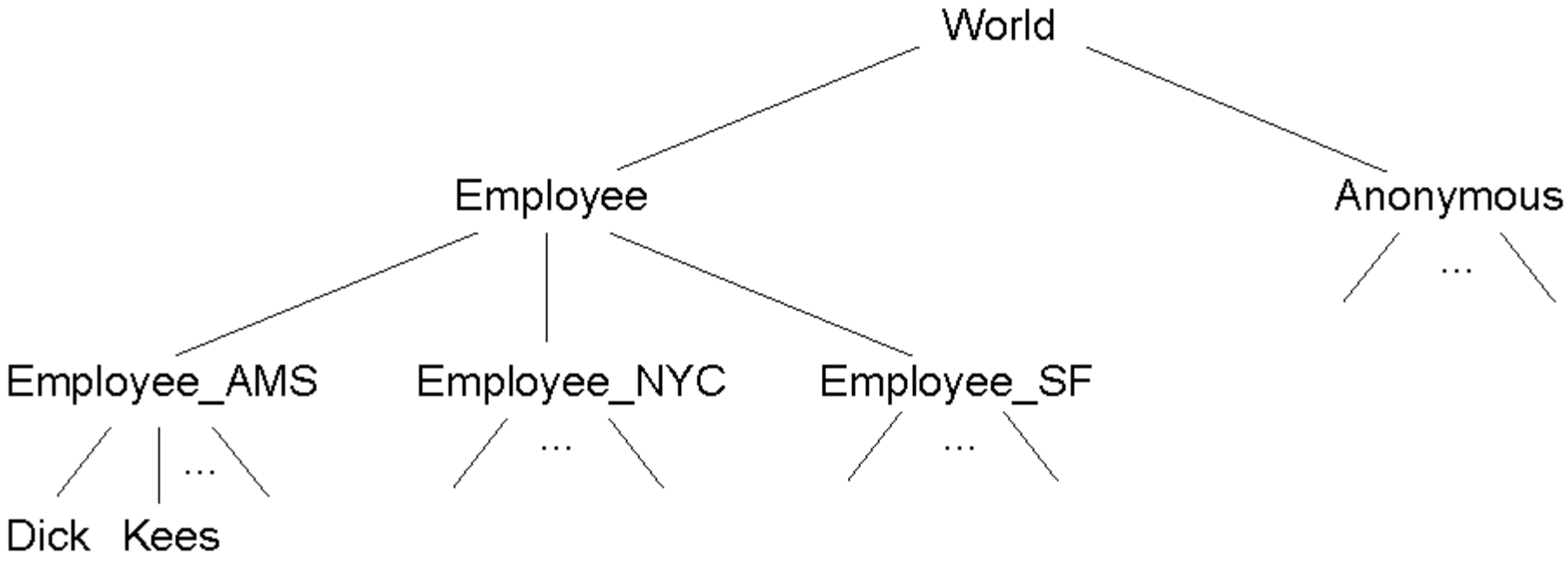


(a)



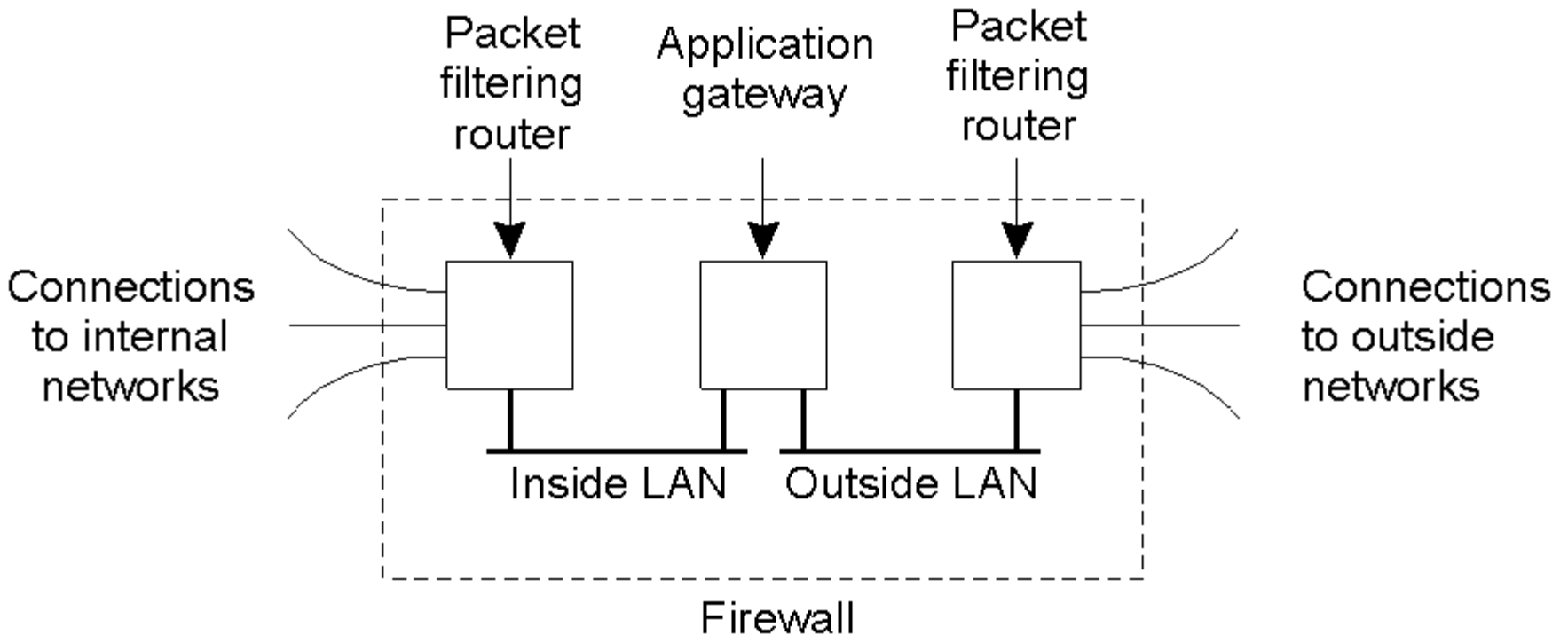
(b)

Protection Domains



The hierarchical organization of protection domains as groups of users.

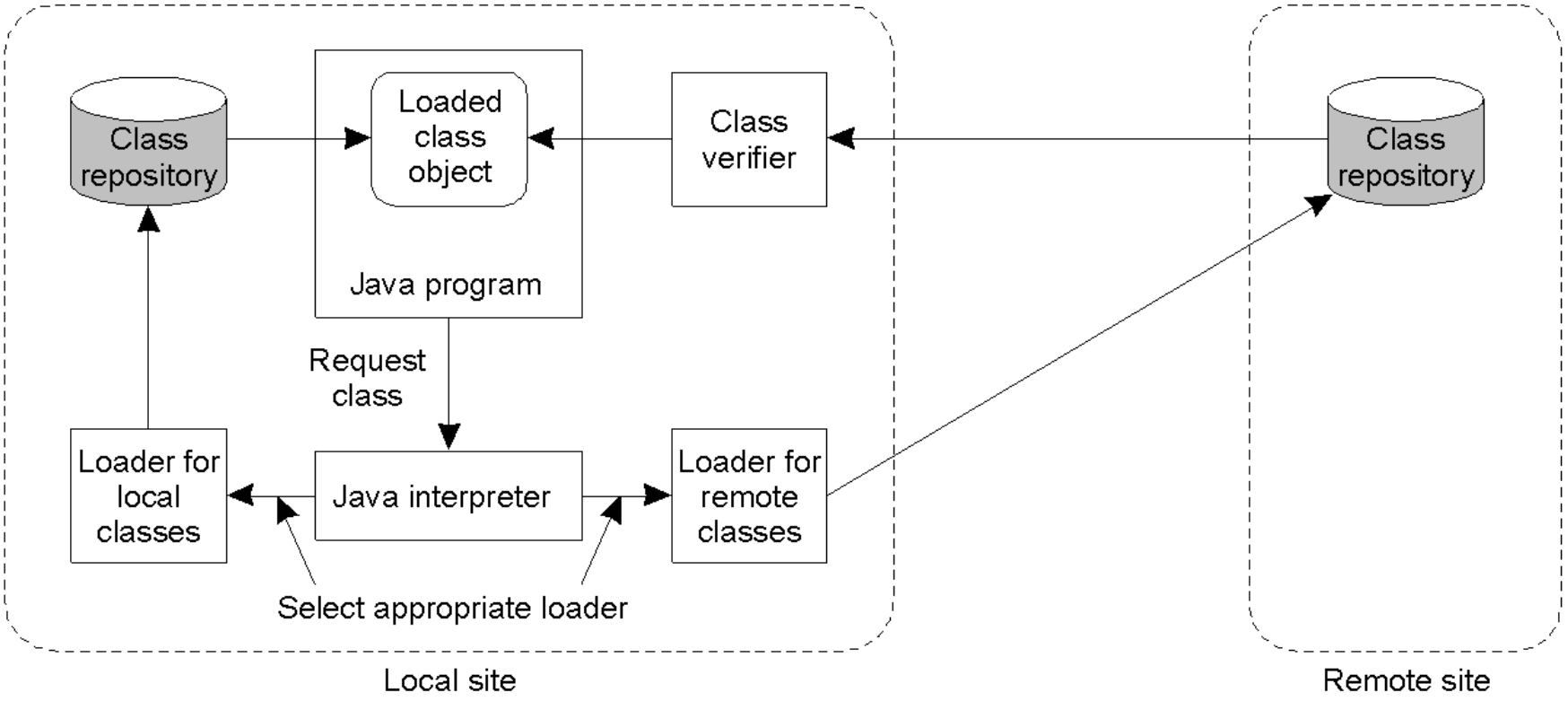
Firewalls



A common implementation of a firewall.

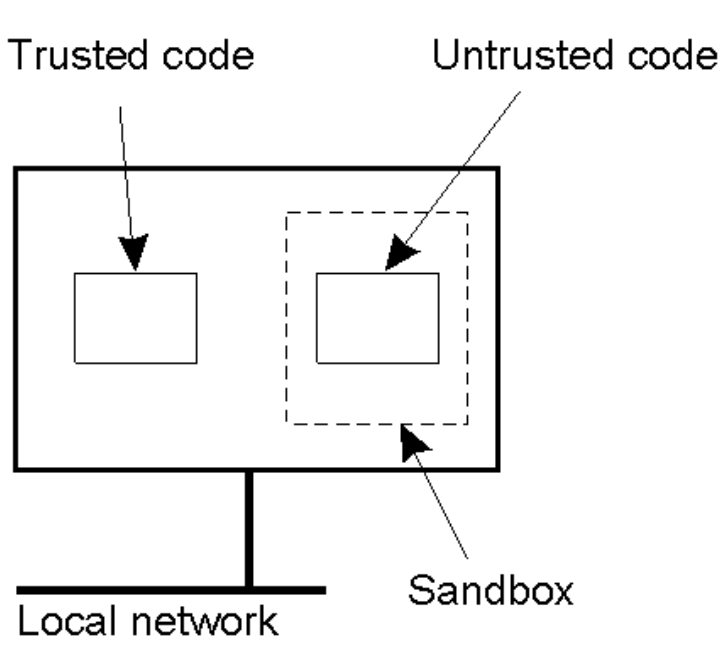
TERIMA KASIH

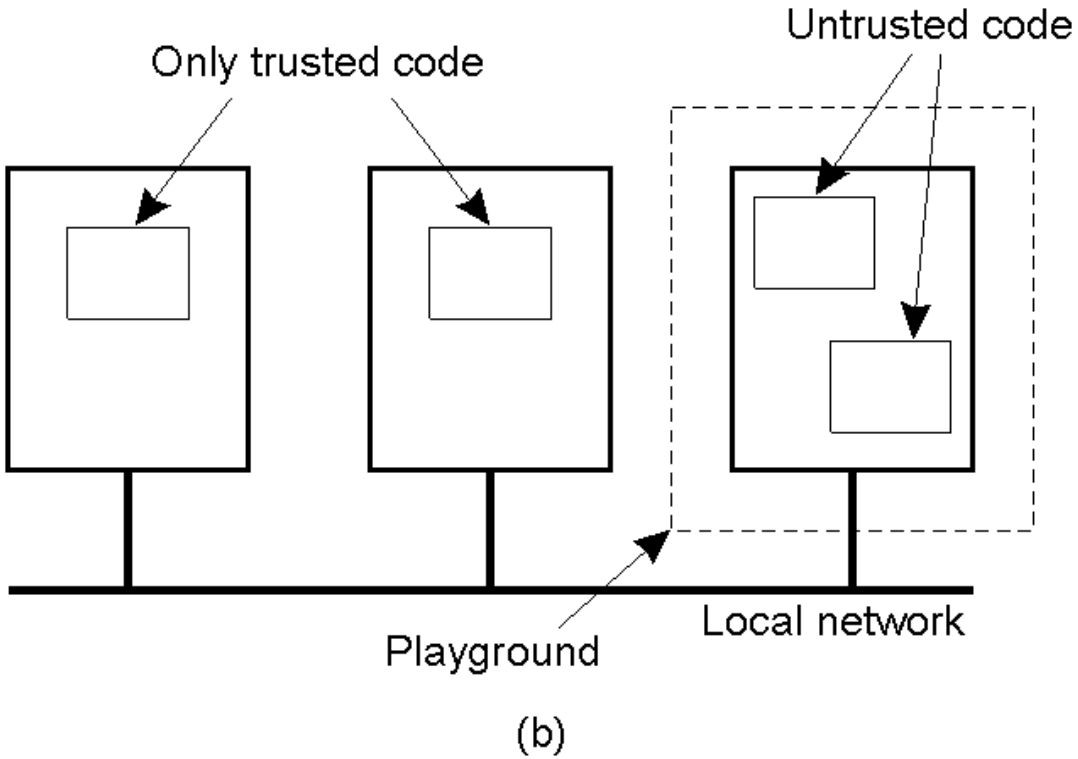
Protecting the Target (1)



The organization of a Java sandbox.

Protecting the Target (2)

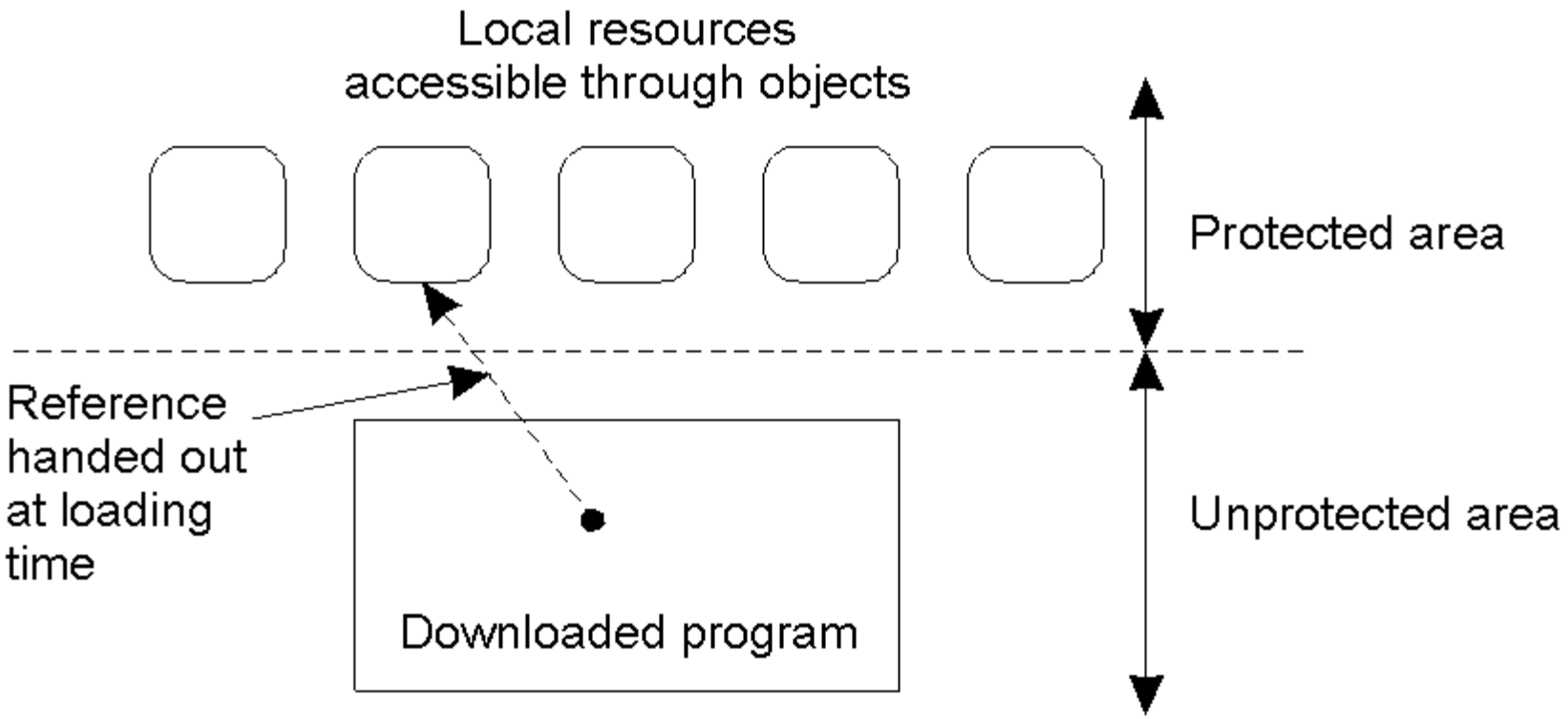




a) A sandbox

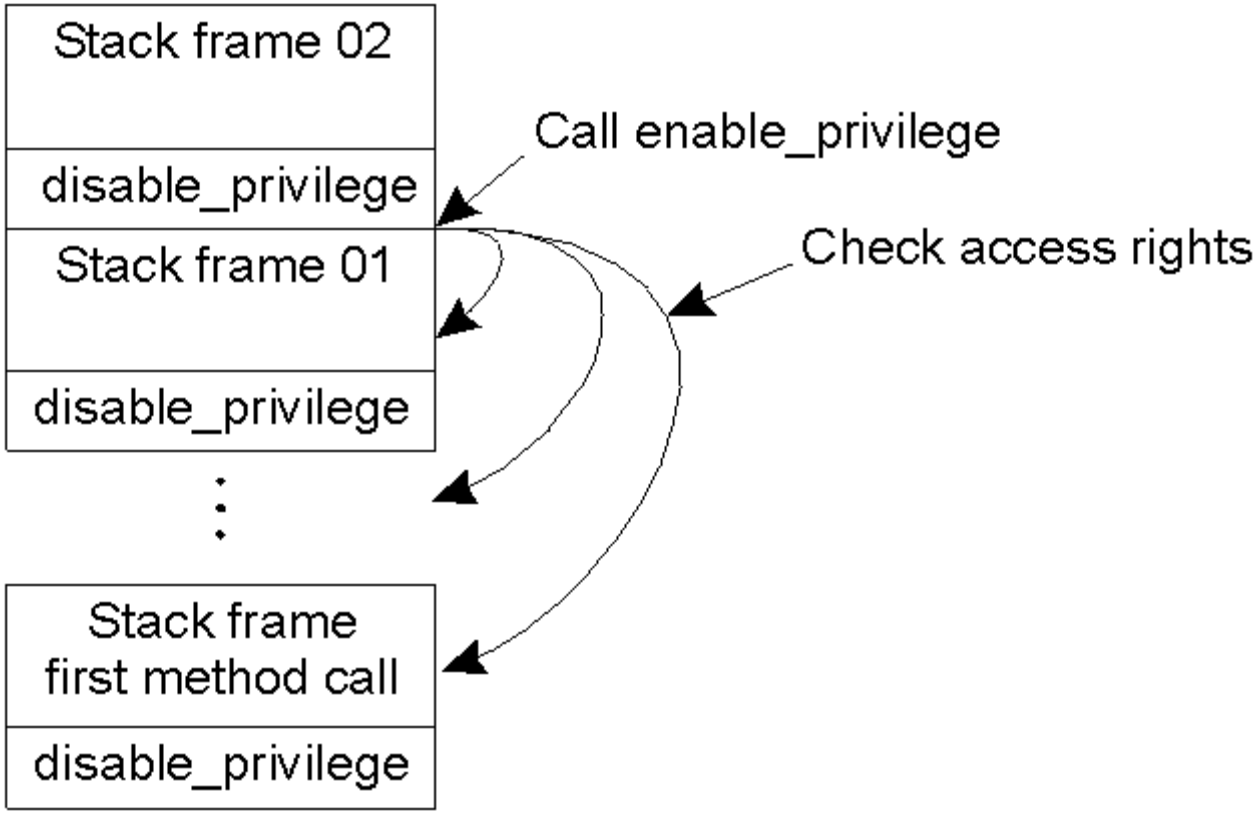
b) A playground

Protecting the Target (3)



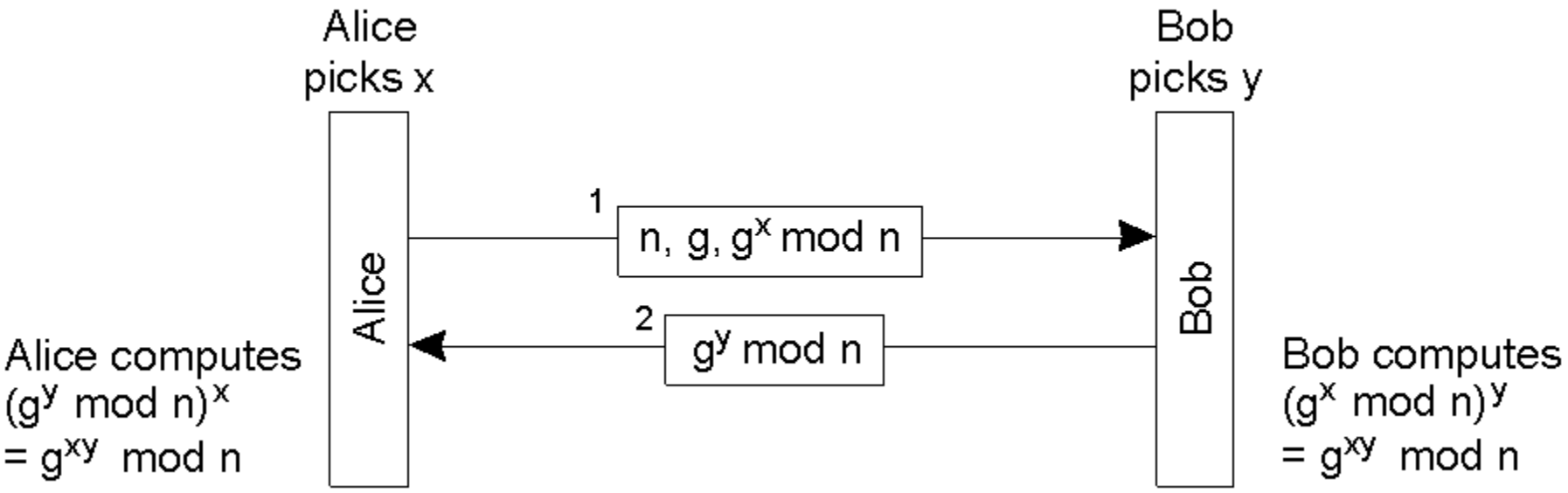
The principle of using Java object references as capabilities.

Protecting the Target (4)



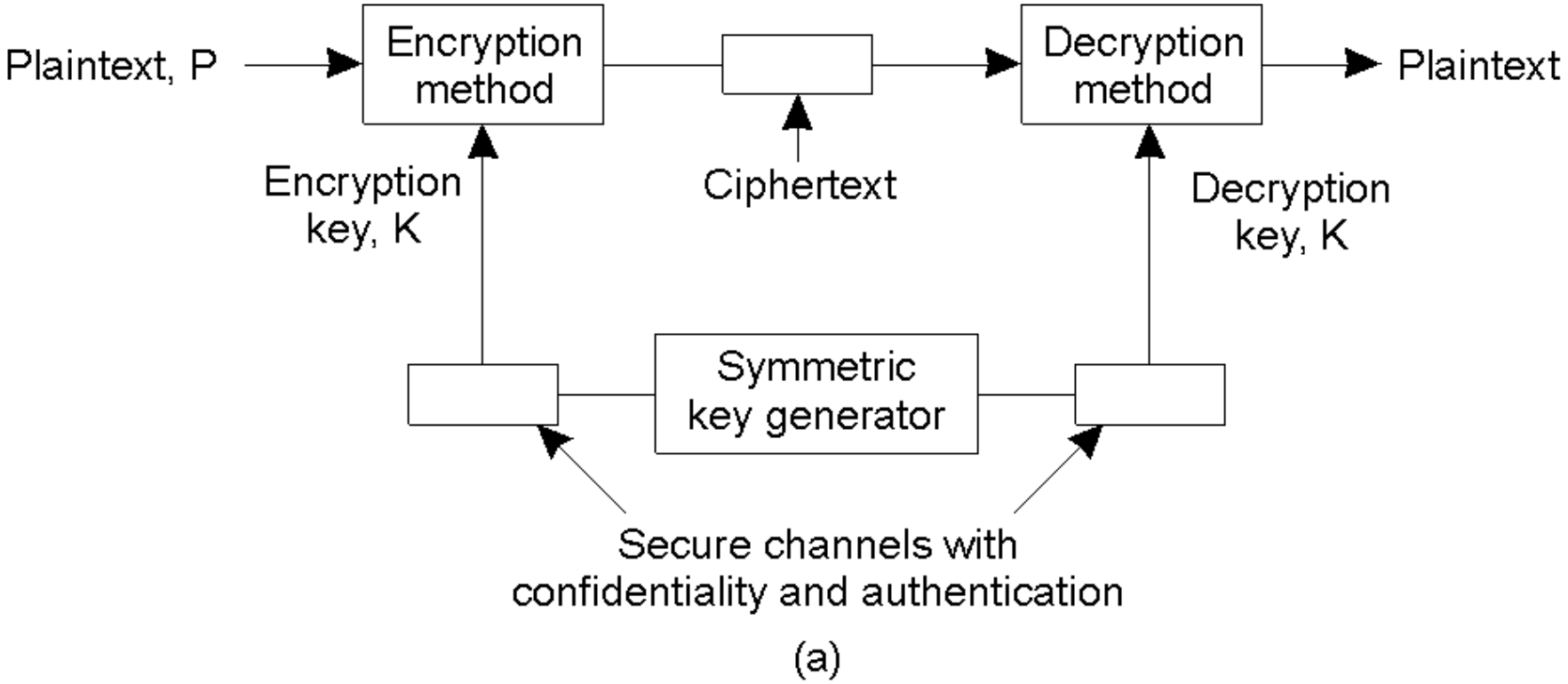
The principle of stack introspection.

SECURE MANAGEMENT
Key Management ->Key Establishment



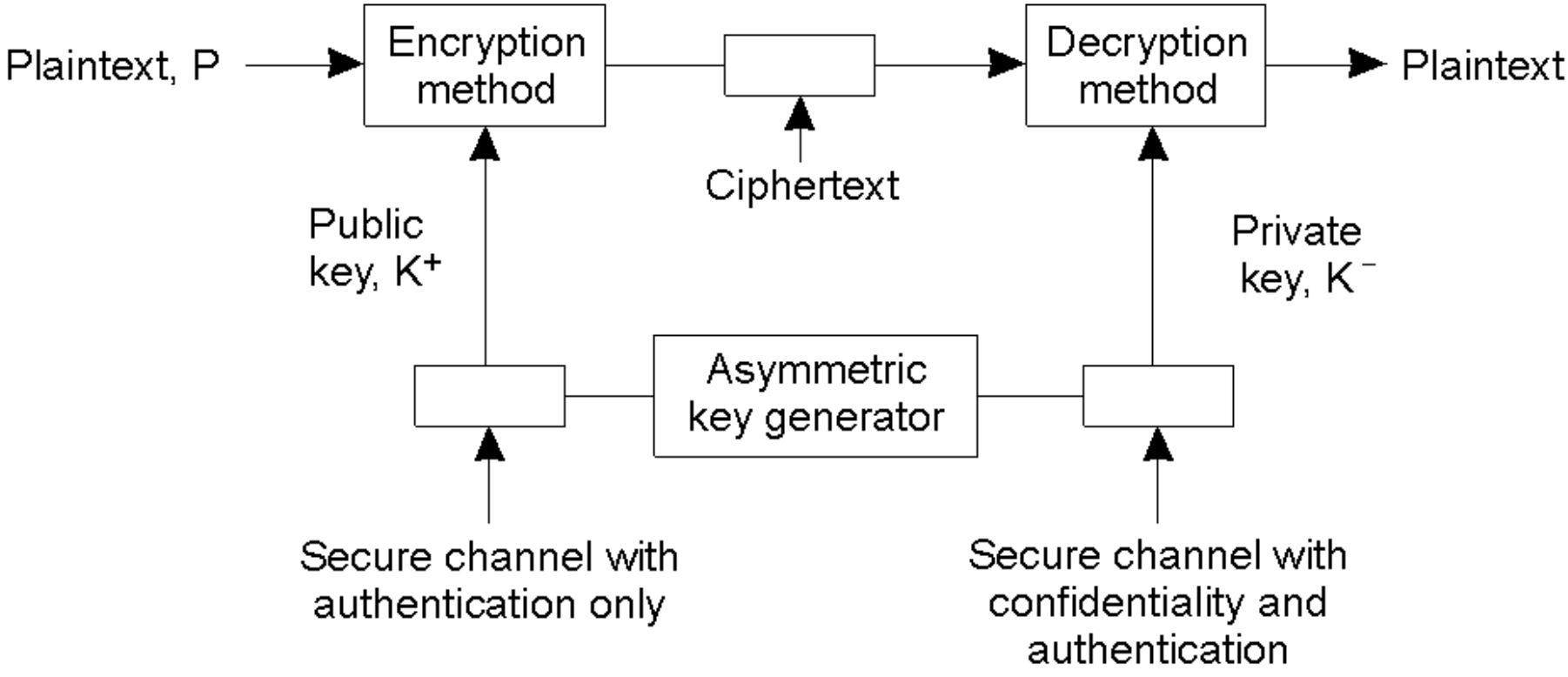
The principle of Diffie-Hellman key exchange.

Key Distribution (1)



Secret-key distribution

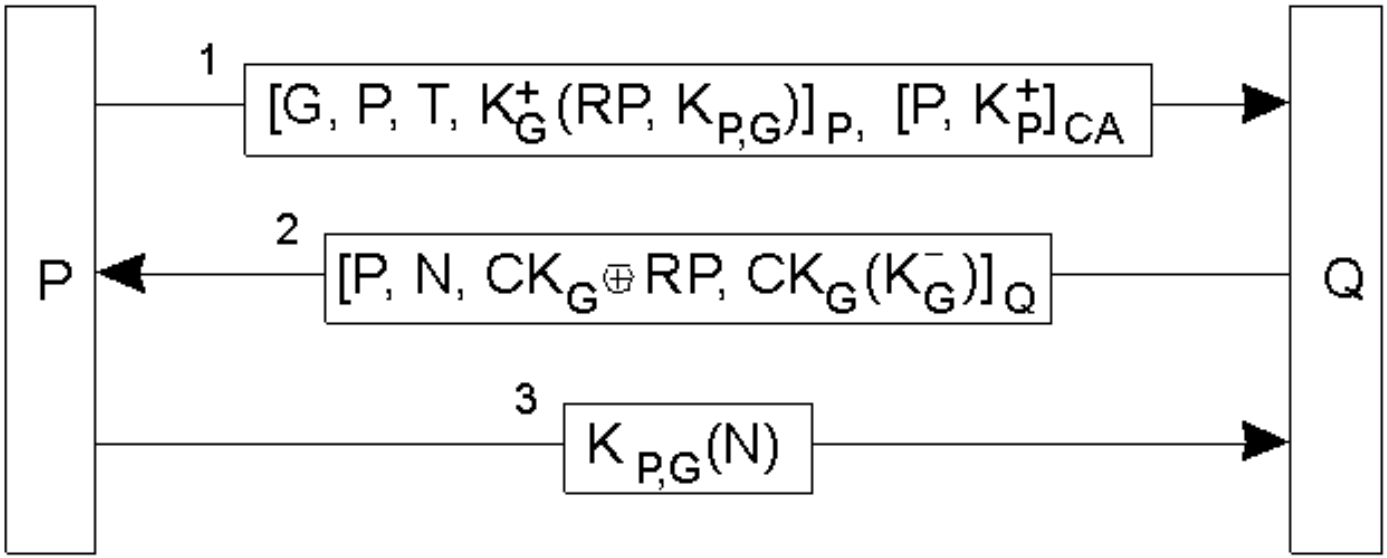
Key Distribution (2)



(b)

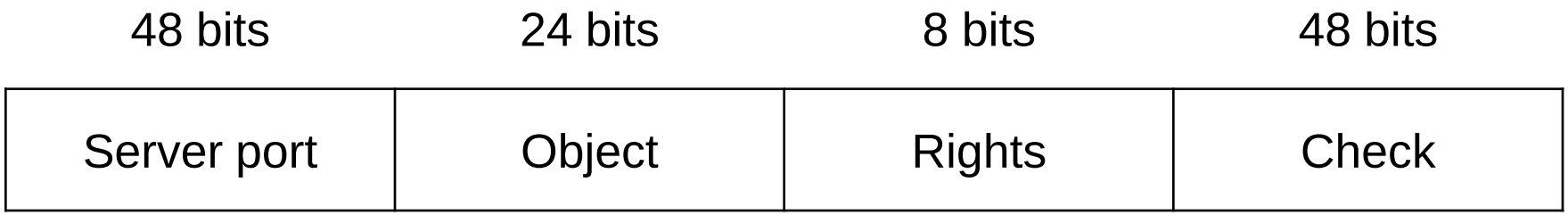
Public-key distribution (see also [menezes.a96]).

Secure Group Management



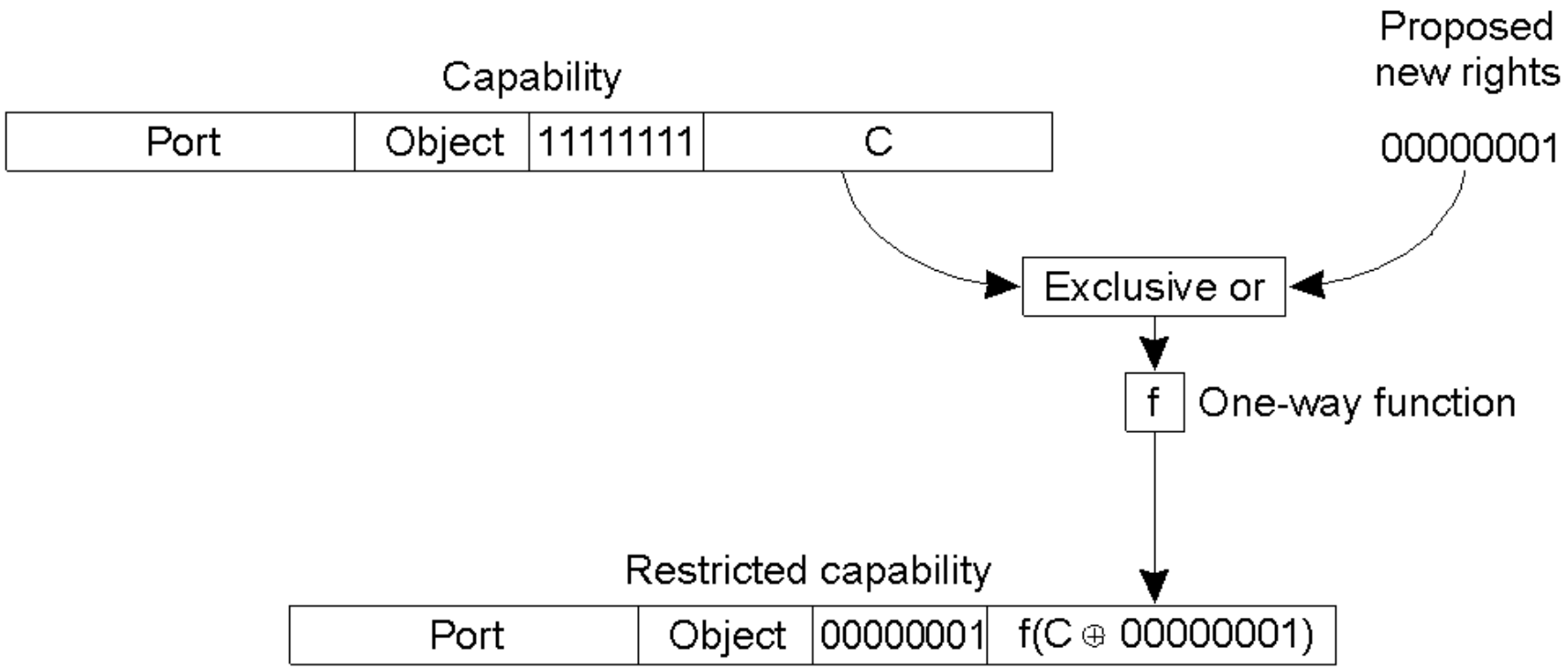
Securely admitting a new group member.

Capabilities and Attribute Certificates (1)



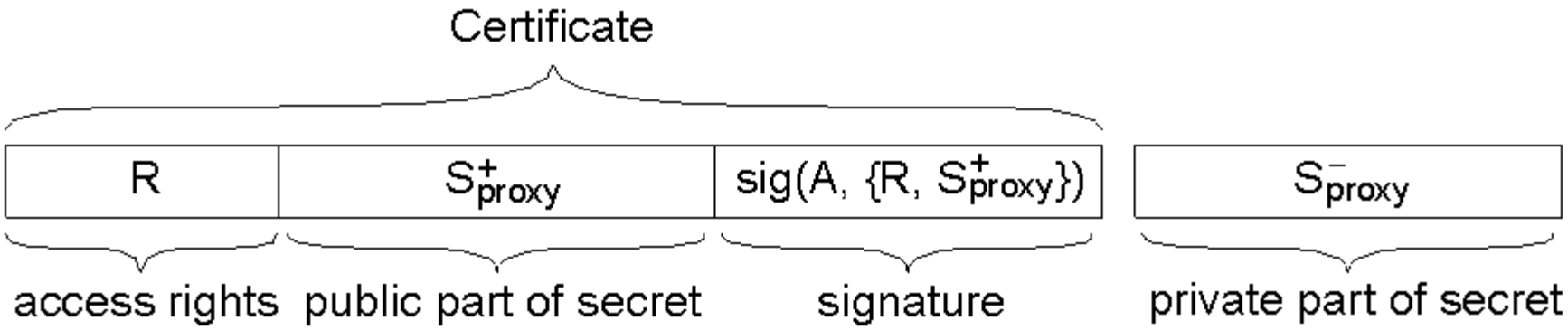
A capability in Amoeba.

Capabilities and Attribute Certificates (2)



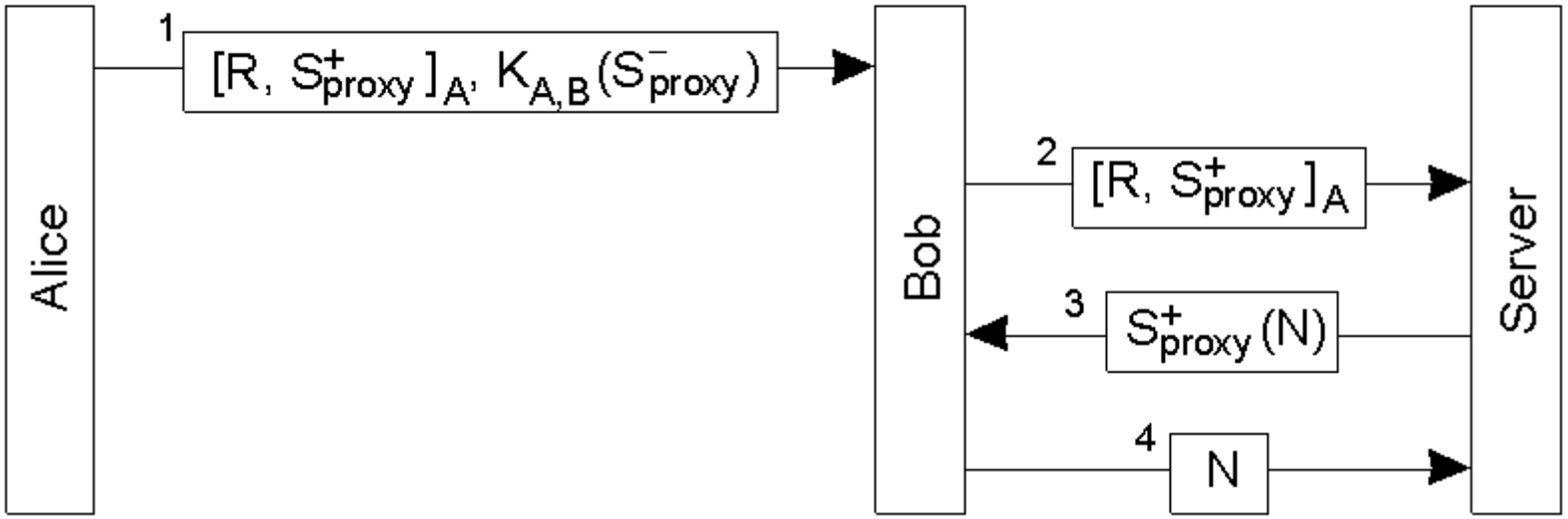
Generation of a restricted capability from an owner capability.

Delegation (1)



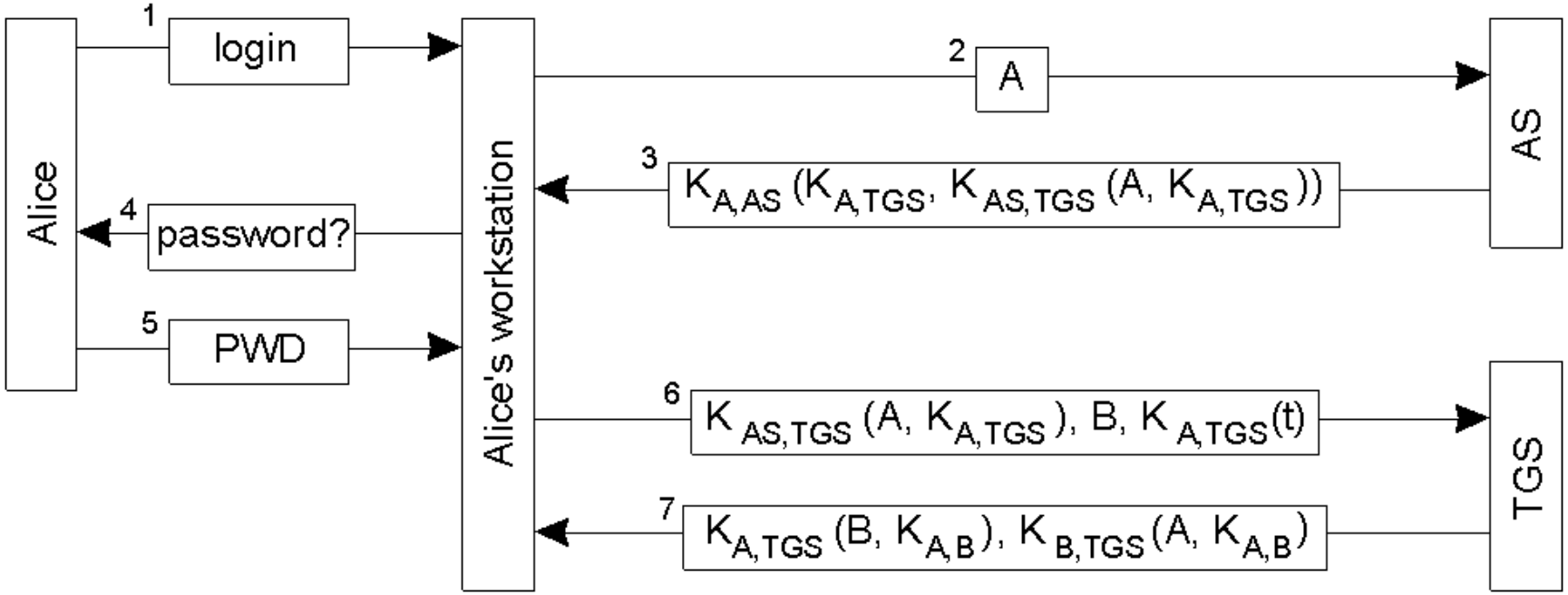
The general structure of a proxy as used for delegation.

Delegation (2)



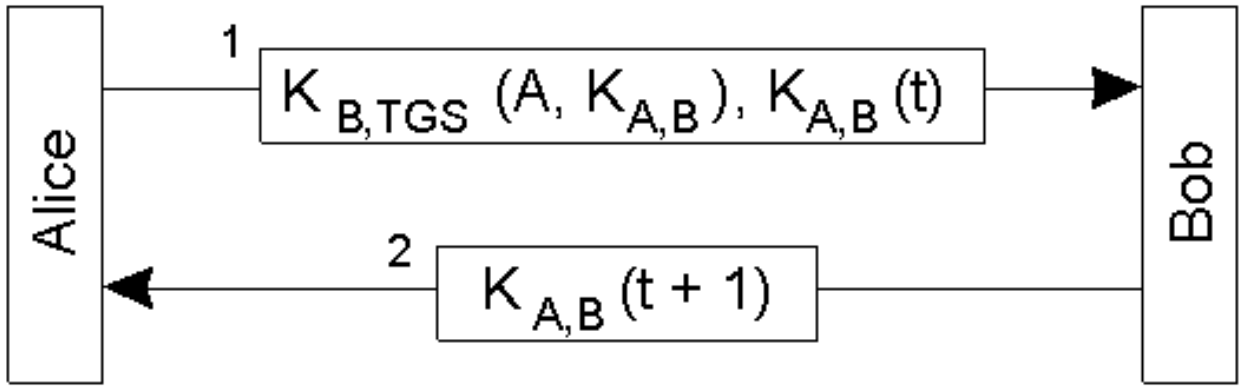
Using a proxy to delegate and prove ownership of access rights.

Example: Kerberos (1)



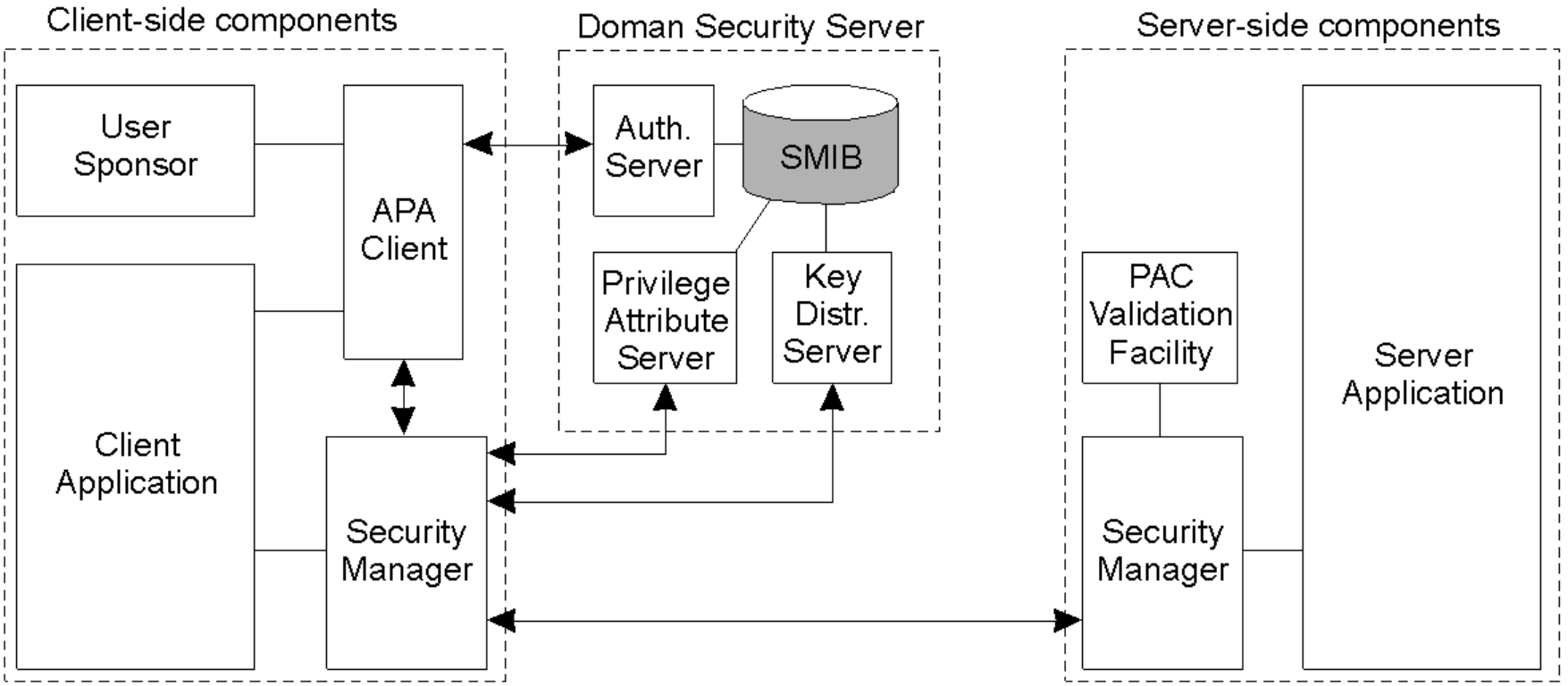
Authentication in Kerberos.

Example: Kerberos (2)



Setting up a secure channel in Kerberos.

SESAME Components



Overview of components in SESAME.

Privilege Attribute Certificates (PACs)

Field	Description
Issuer domain	Name the security domain of the issuer
Issuer identity	Name the PAS in the issuer's domain
Serial number	A unique number for this PAC, generated by the PAS
Creation time	UTC time when this PAC was created
Validity	Time interval when this PAC is valid
Time periods	Additional time periods outside which the PAC is invalid
Algorithm ID	Identifier of the algorithm used to sign this PAC
Signature value	The signature placed on the PAC
Privileges	A list of (attribute, value)-pairs describing privileges
Certificate information	Additional information to be used by the PVF
Miscellaneous	Currently used for auditing purposes only
Protection methods	Fields to control how the PAC i s used

The organization of a SESAME Privilege Attribute Certificate.

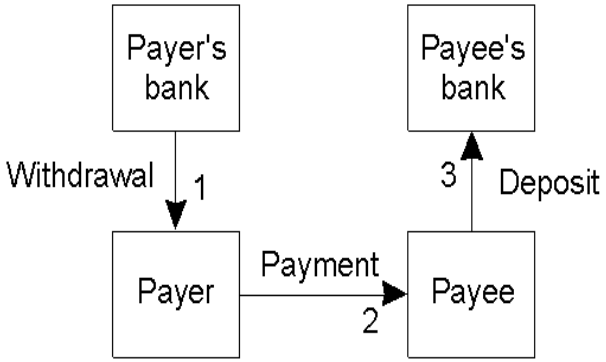
Electronic Payment Systems (1)

Payment systems based on direct payment between customer and merchant.

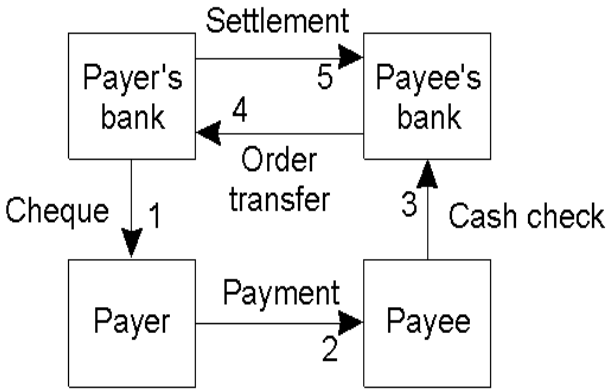
a) Paying in cash.

b) Using a check.

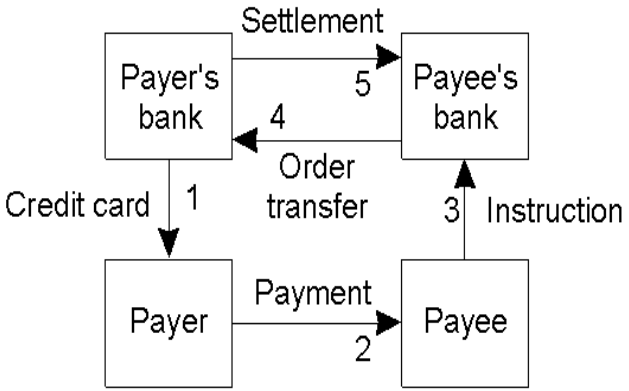
c) Using a credit card.



(a)

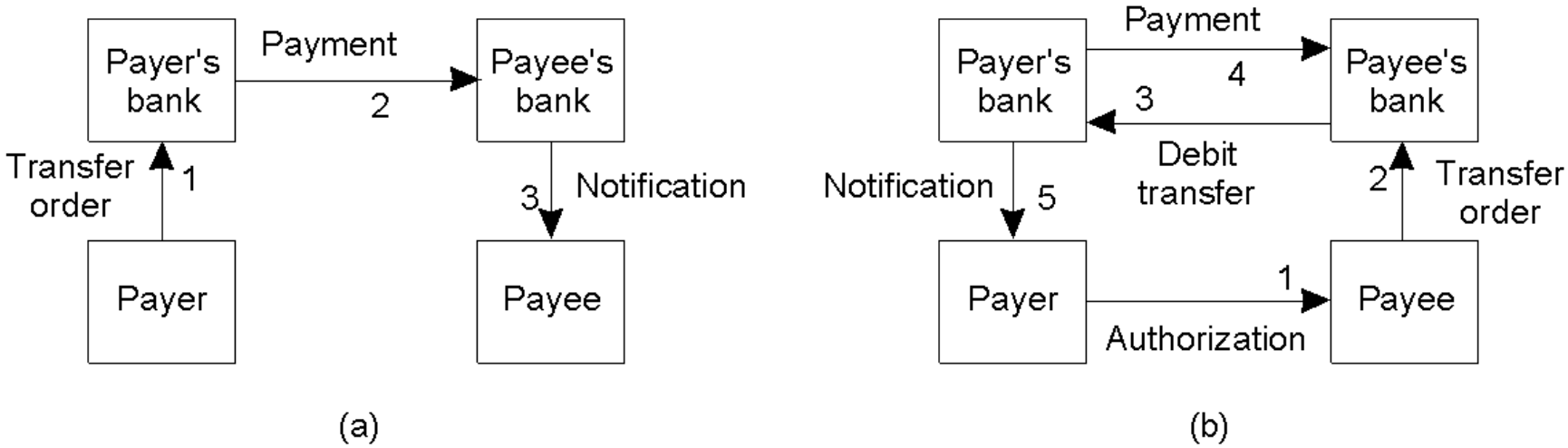


(b)



(c)

Electronic Payment Systems (2)



Payment systems based on money transfer between banks.

a) Payment by money order.

b) Payment through debit order.

Privacy (1)

	Merchant	Customer	Date	Amount	Item
Merchant	Full	Partial	Full	Full	Full
Customer	Full	Full	Full	Full	Full
Bank	None	None	None	None	None
Observer	Full	Partial	Full	Full	Full

Information hiding in a traditional cash payment.

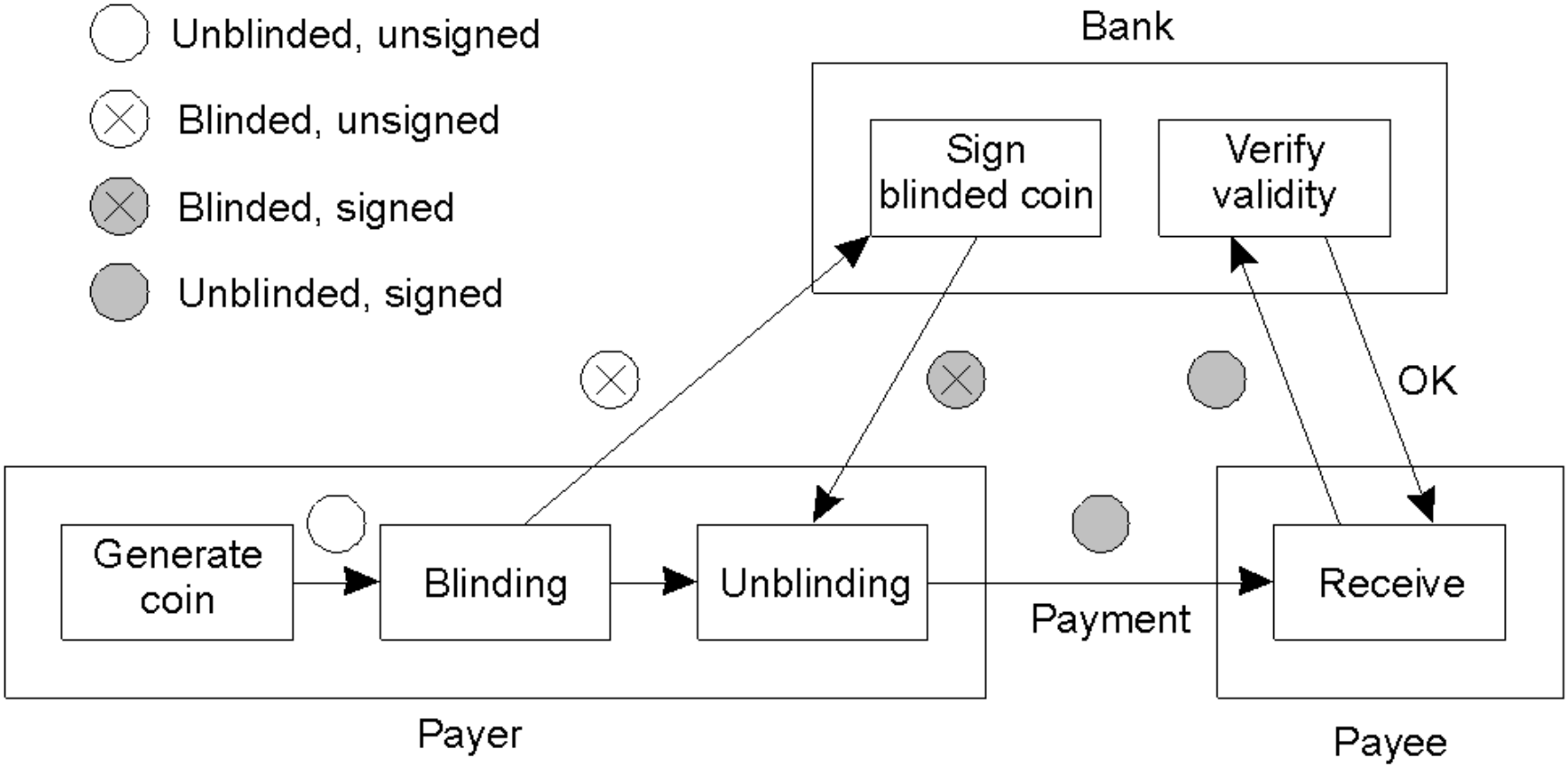
Privacy (2)

Information

Party	Merchant	Customer	Date	Amount	Item
Merchant	Full	Full	Full	Full	Full
Customer	Full	Full	Full	Full	Full
Bank	Full	Full	Full	Full	None
Observer	Full	Partial	Full	Full	Full

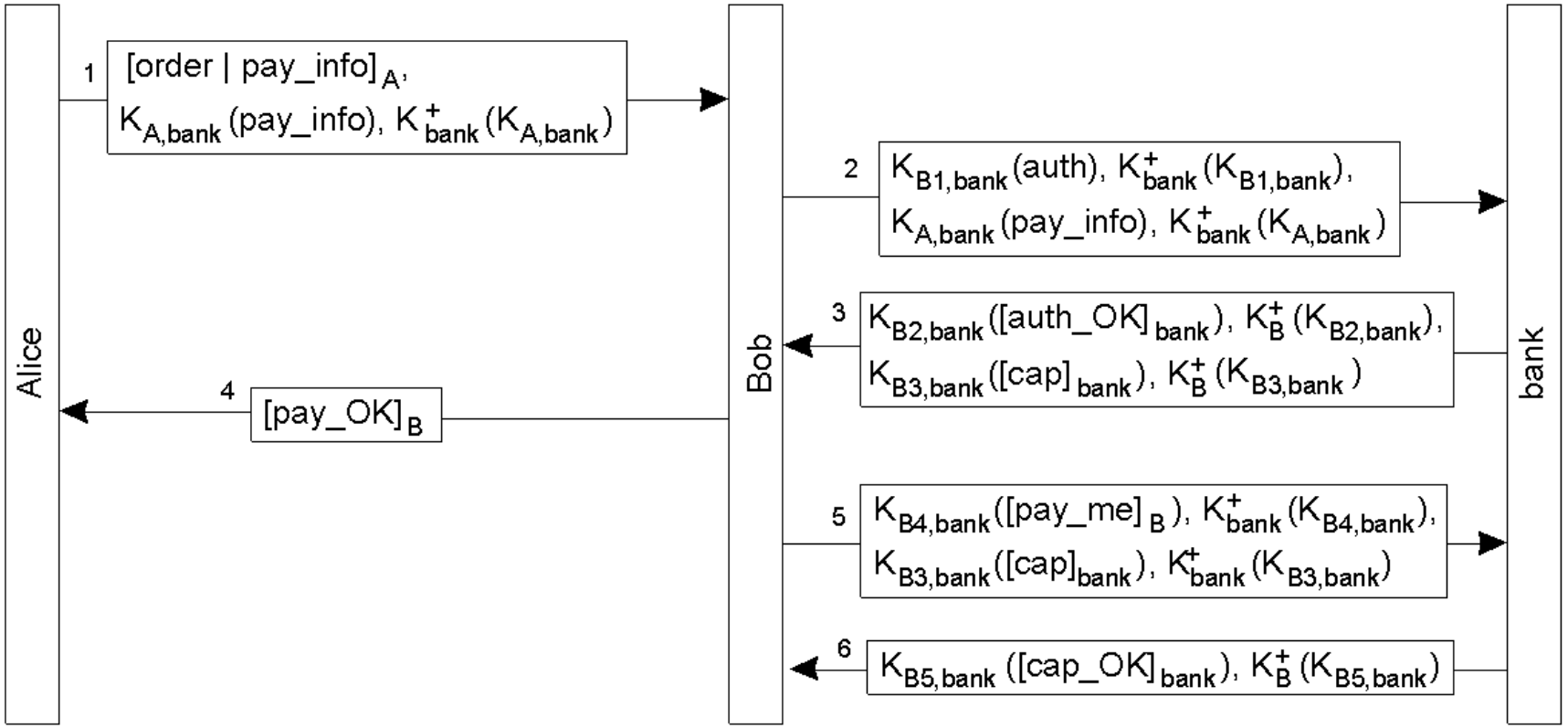
Information hiding in a traditional credit-card system (see also [camp.lj96a])

E-cash



The principle of anonymous electronic cash using blind signatures.

Secure Electronic Transactions (SET)



The different steps in SET.