Распределенные системы

Безопасность

Types of Threats

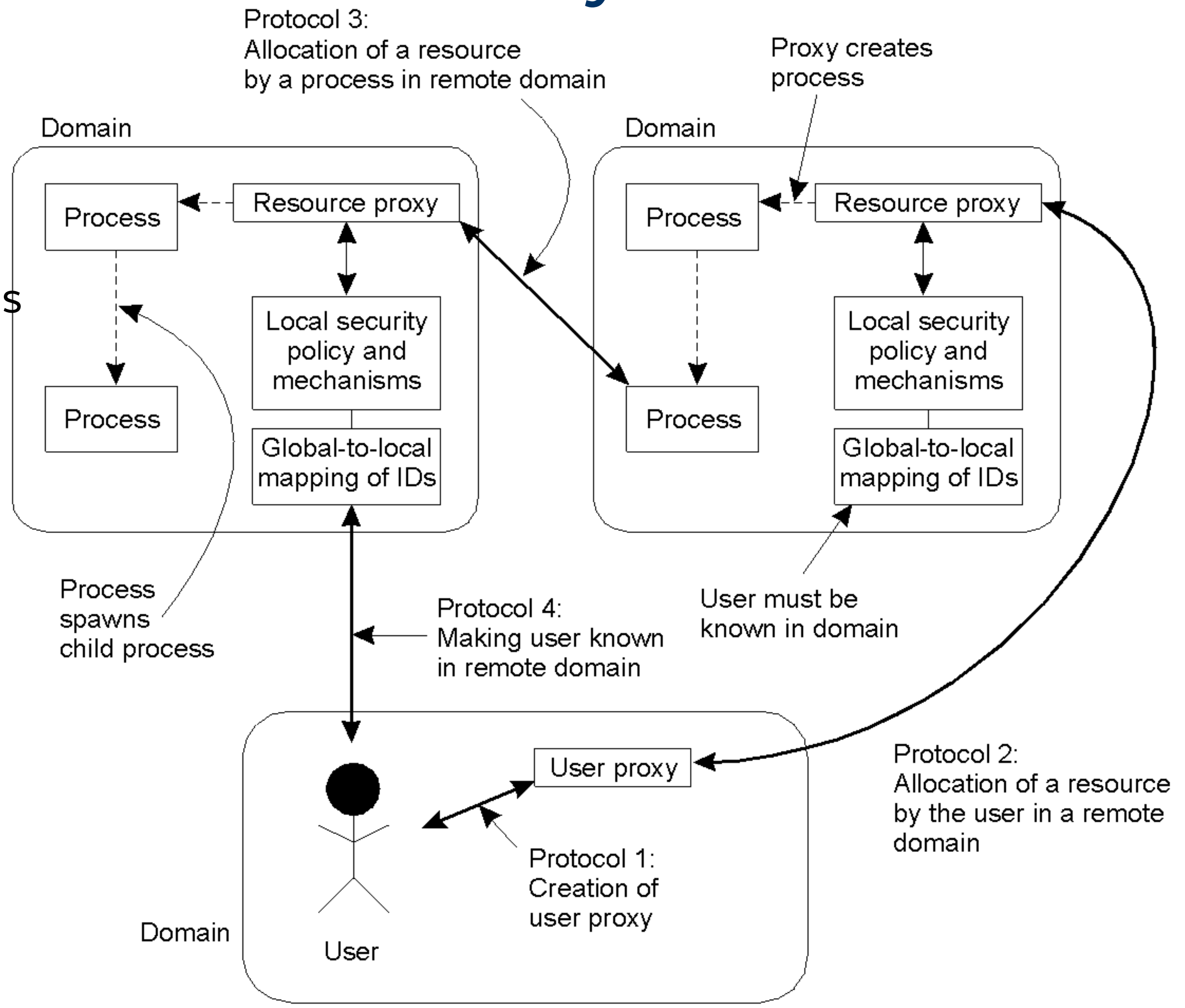
- Interception
- Interruption
- Modification
- Fabrication

Security Mechanisms

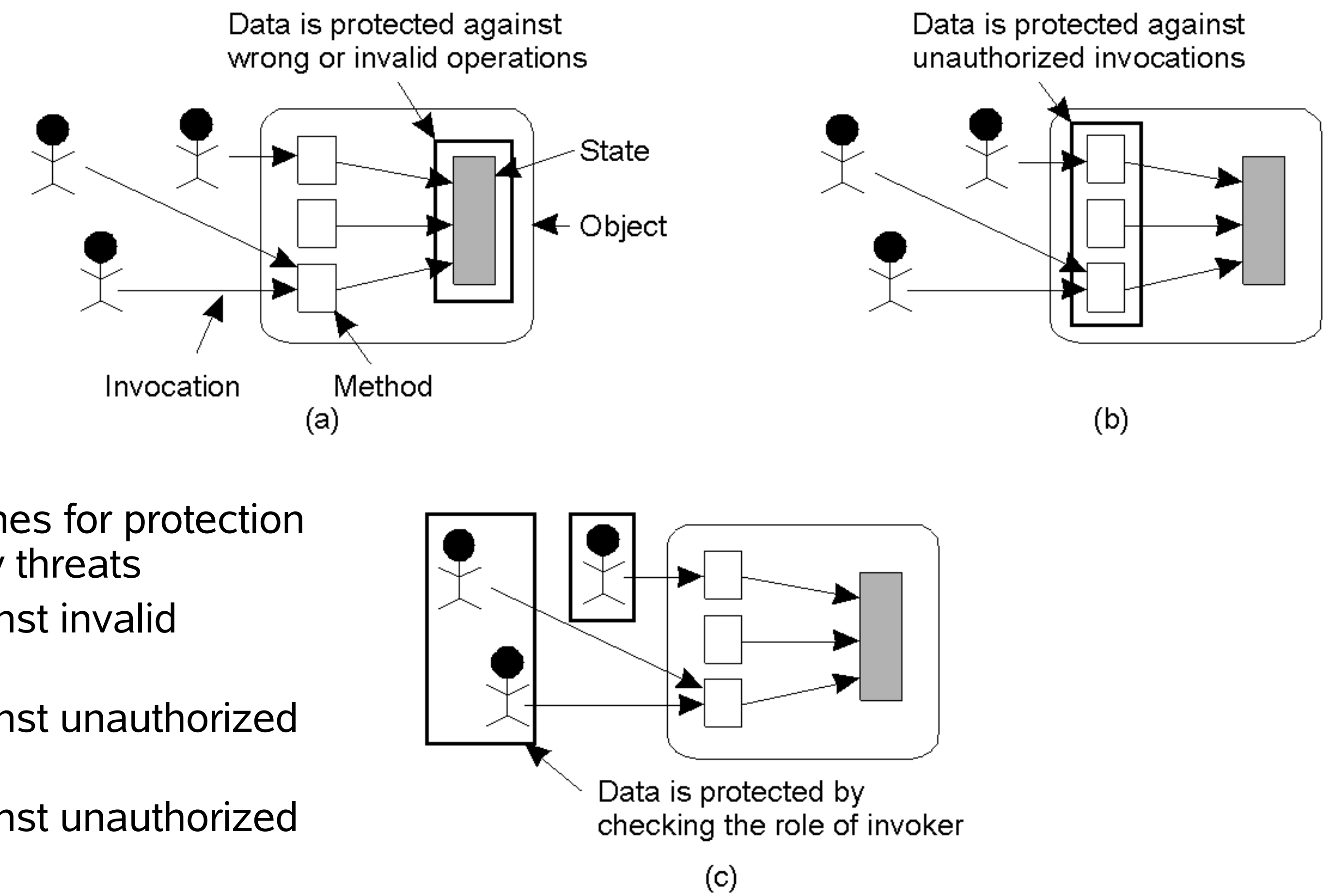
- Encryption
- Authentication
- Authorization
- Auditing

Example: Globus Security Architecture

- Diagram of Globus security architecture.



Focus of Control


Data is protected against wrong or invalid operations
State
Object
Invocation
Method
(a)
Data is protected against unauthorized invocations
(b)
Data is protected by checking the role of invoker
(c)

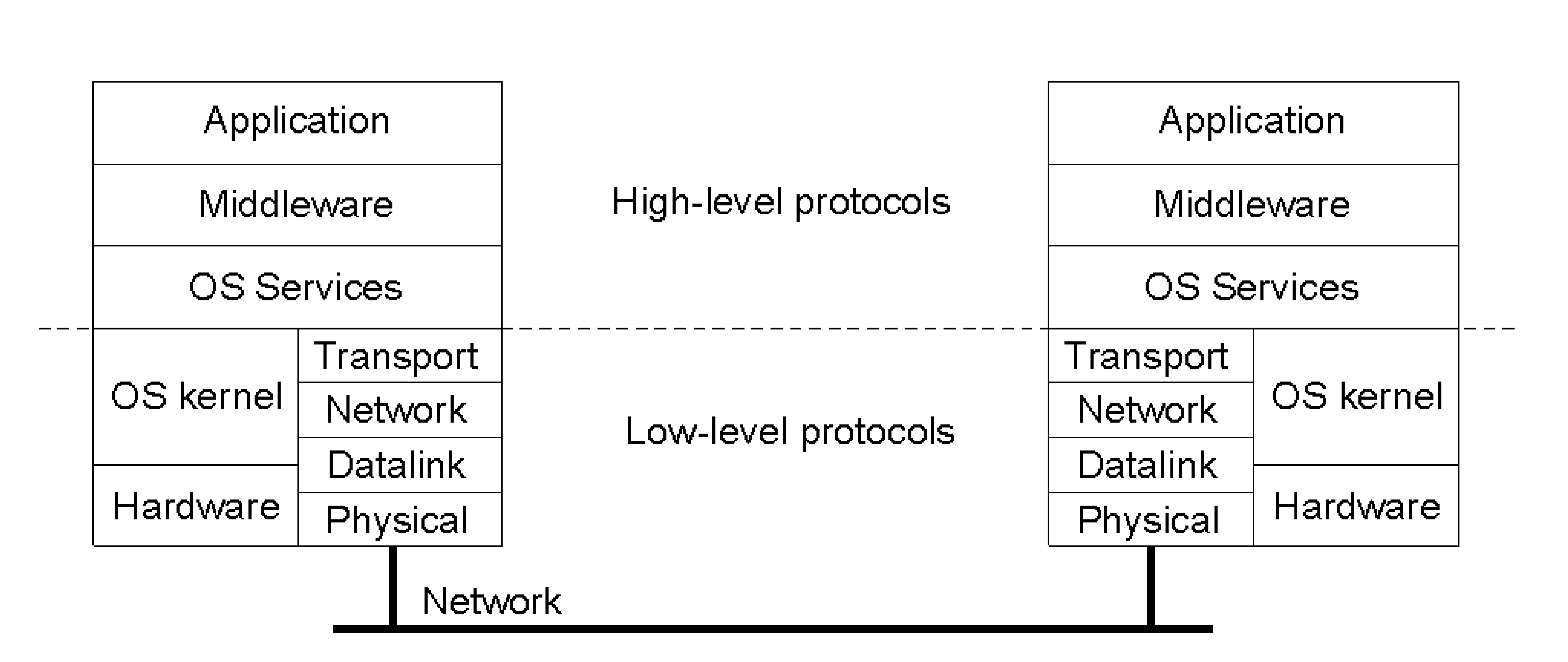
- Three approaches for protection against security threats

a) Protection against invalid operations

b) Protection against unauthorized invocations

c) Protection against unauthorized users

Layering of Security Mechanisms (1)



Application

Middleware

OS Services

OS kernel

Hardware

Transport

Network

Datalink

Physical

High-level protocols

Low-level protocols

Application

Middleware

OS Services

Transport

Network

Datalink

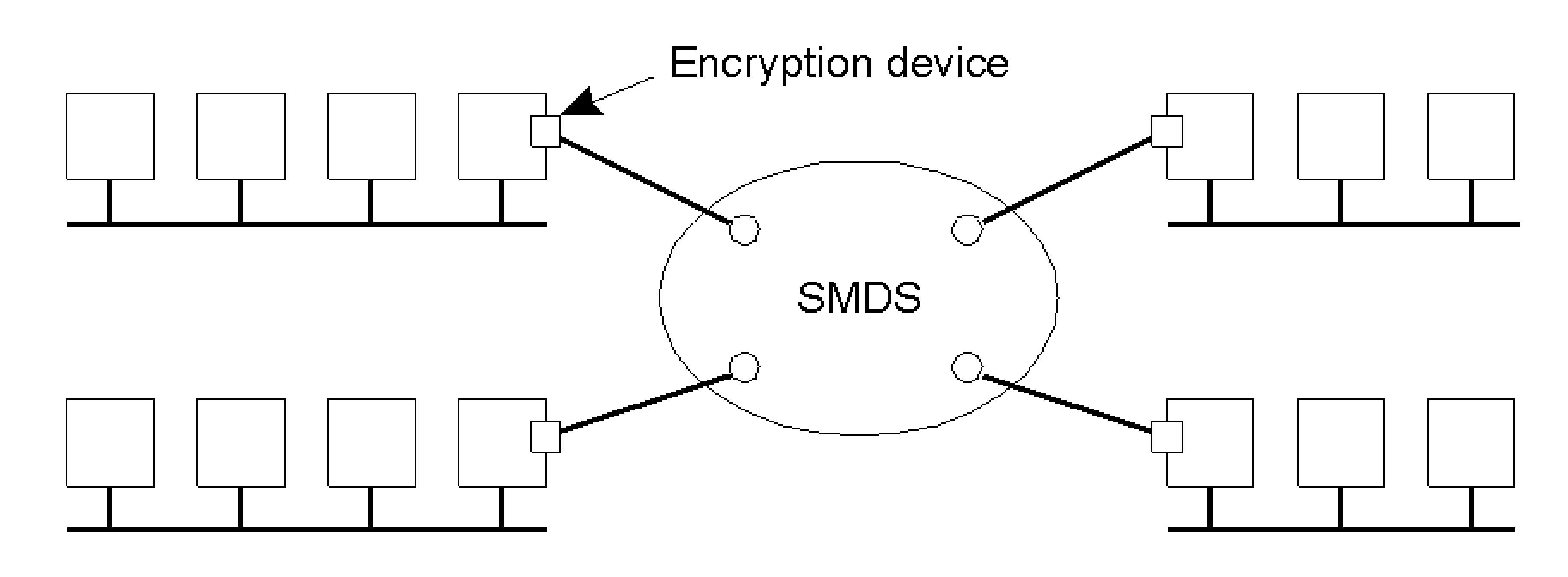
Physical

OS kernel

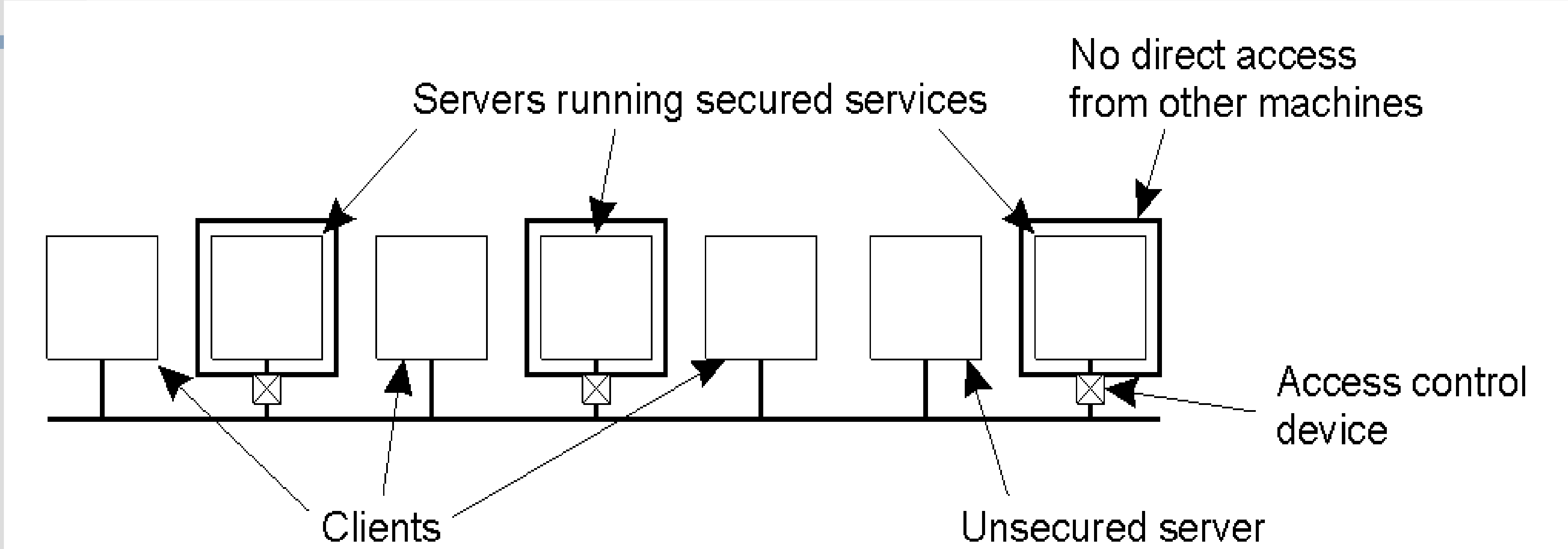
Hardware

Network

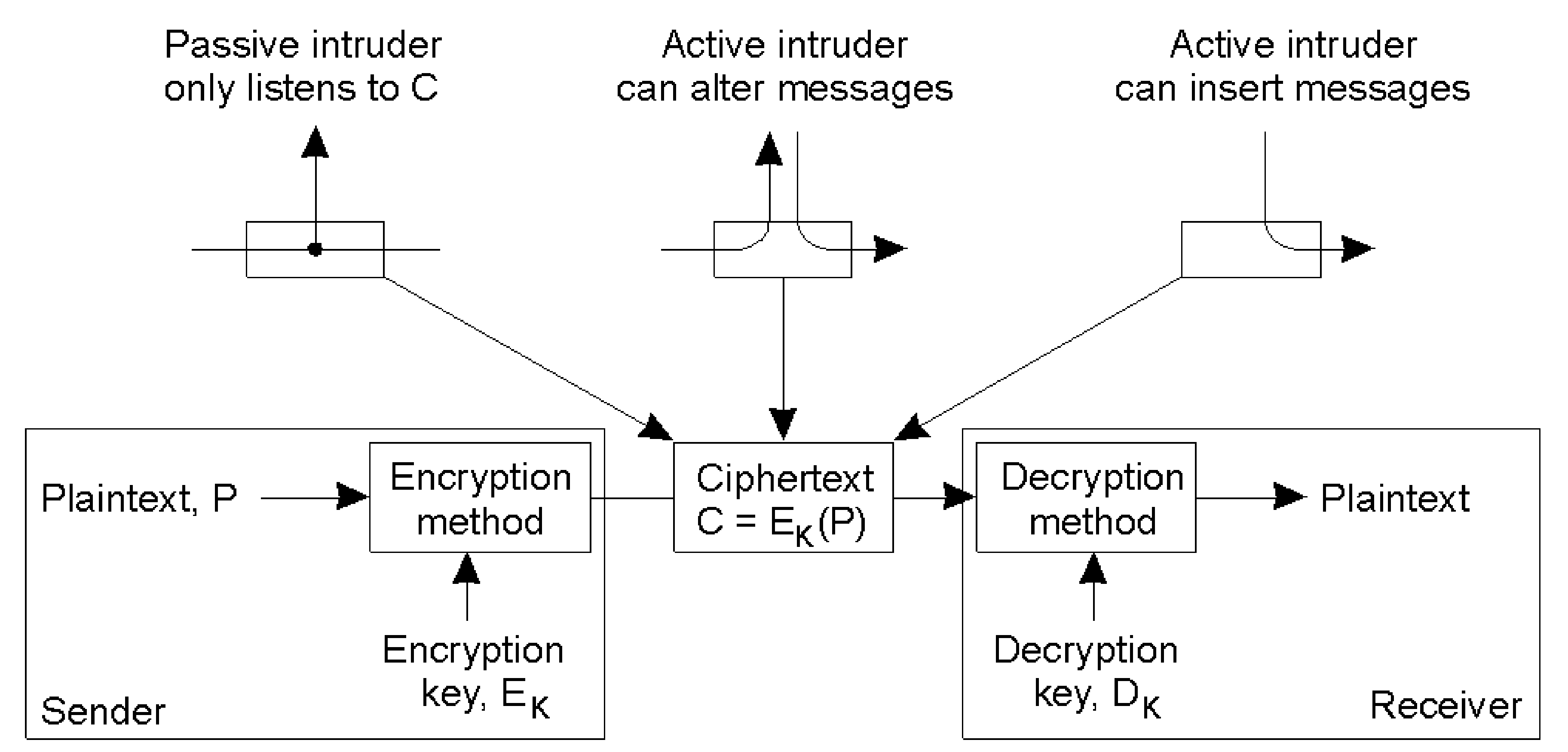
Layering of Security Mechanisms (2)



Distribution of Security Mechanisms


Servers running secured services
No direct access from other machines
Access control device
Clients
Unsecured server

Cryptography (1)

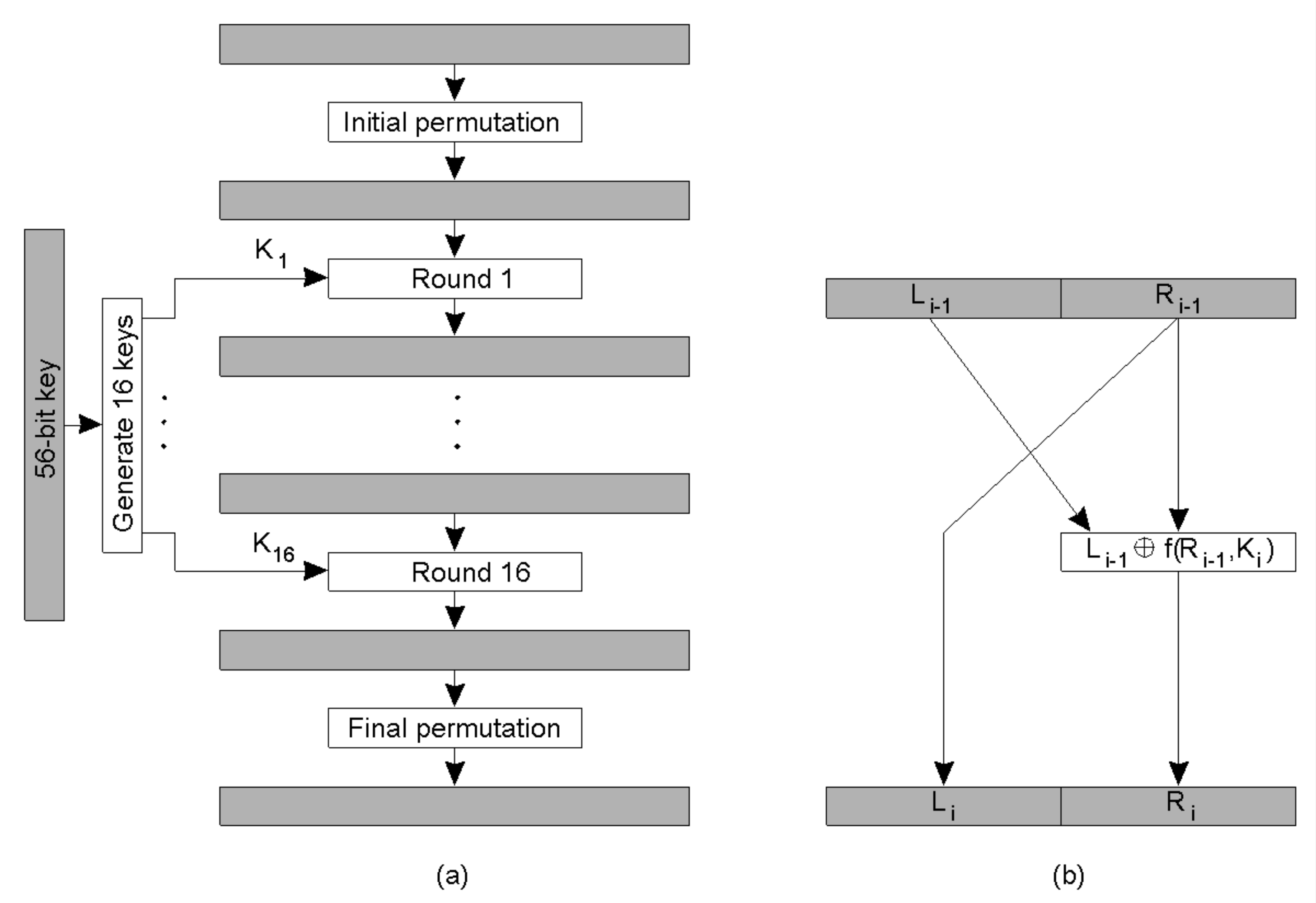


Cryptography (2)

- Notation used in this chapter.

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

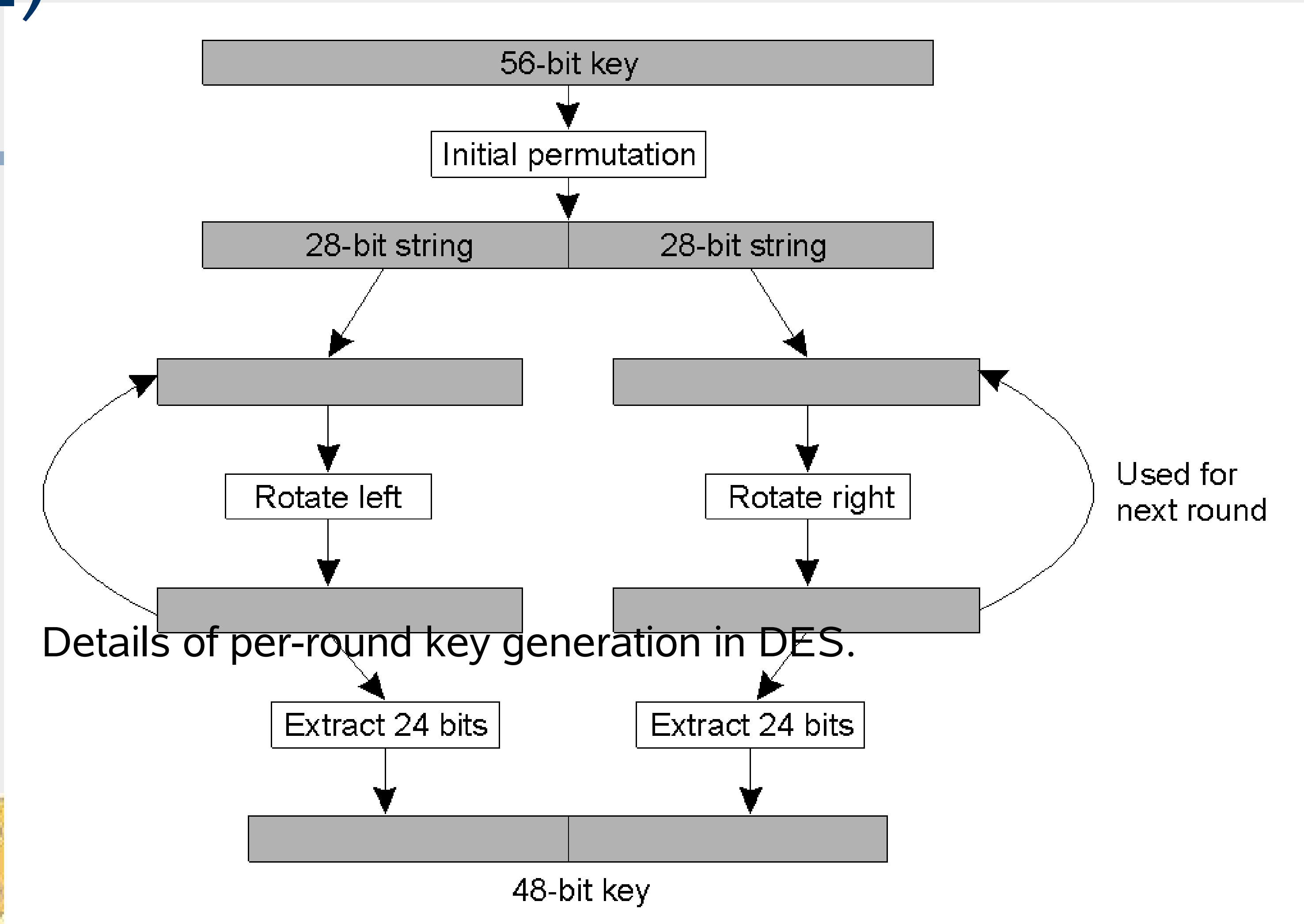
Symmetric Cryptosystems: DES (1)



a) The principle of DES

b) Outline of one encryption round

Symmetric Cryptosystems: DES (2)



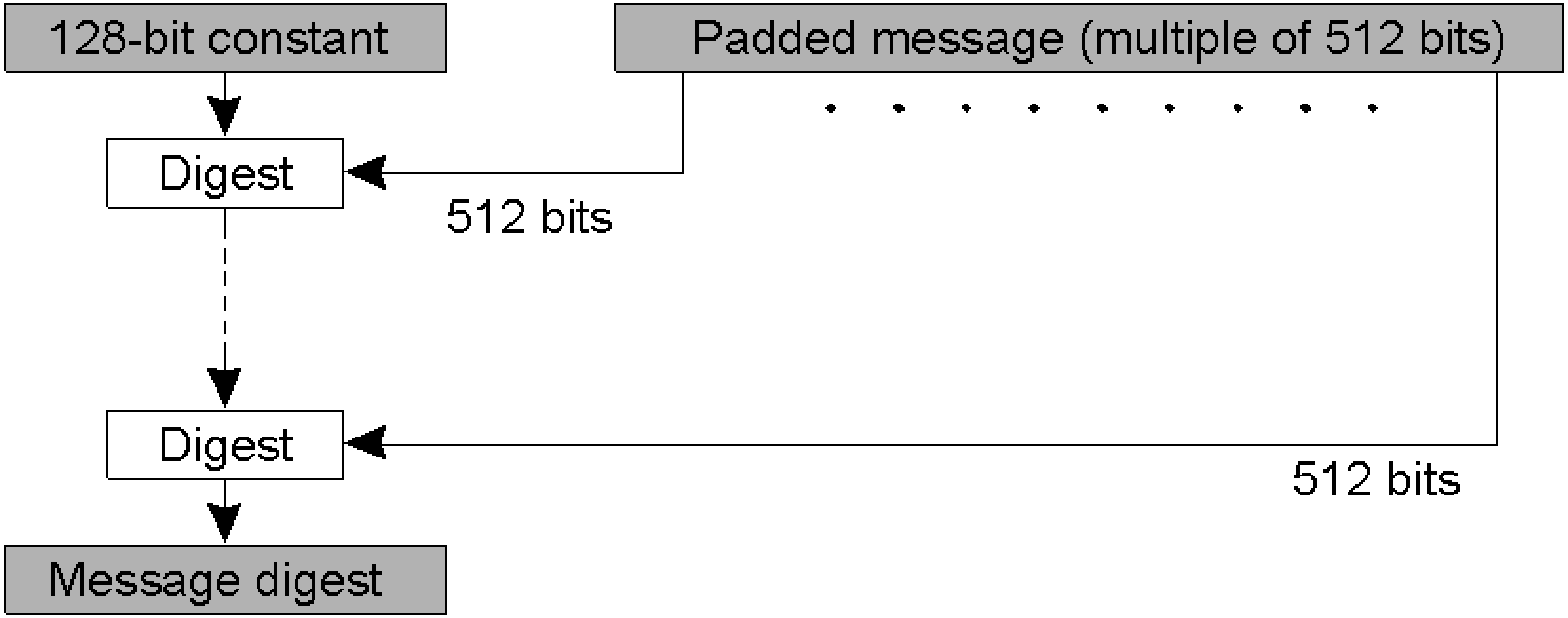
- Details of per-round key generation in DES.

Public-Key Cryptosystems: RSA

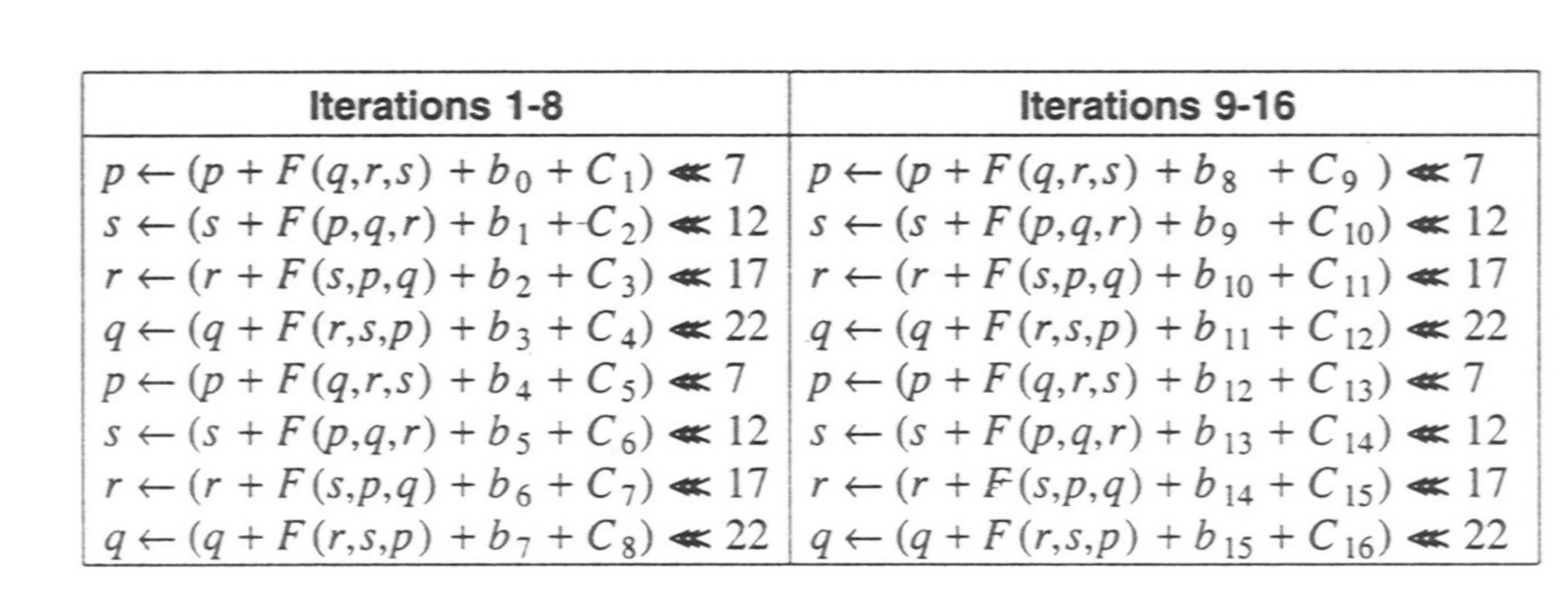
- Generating the private and public key requires four steps:

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)



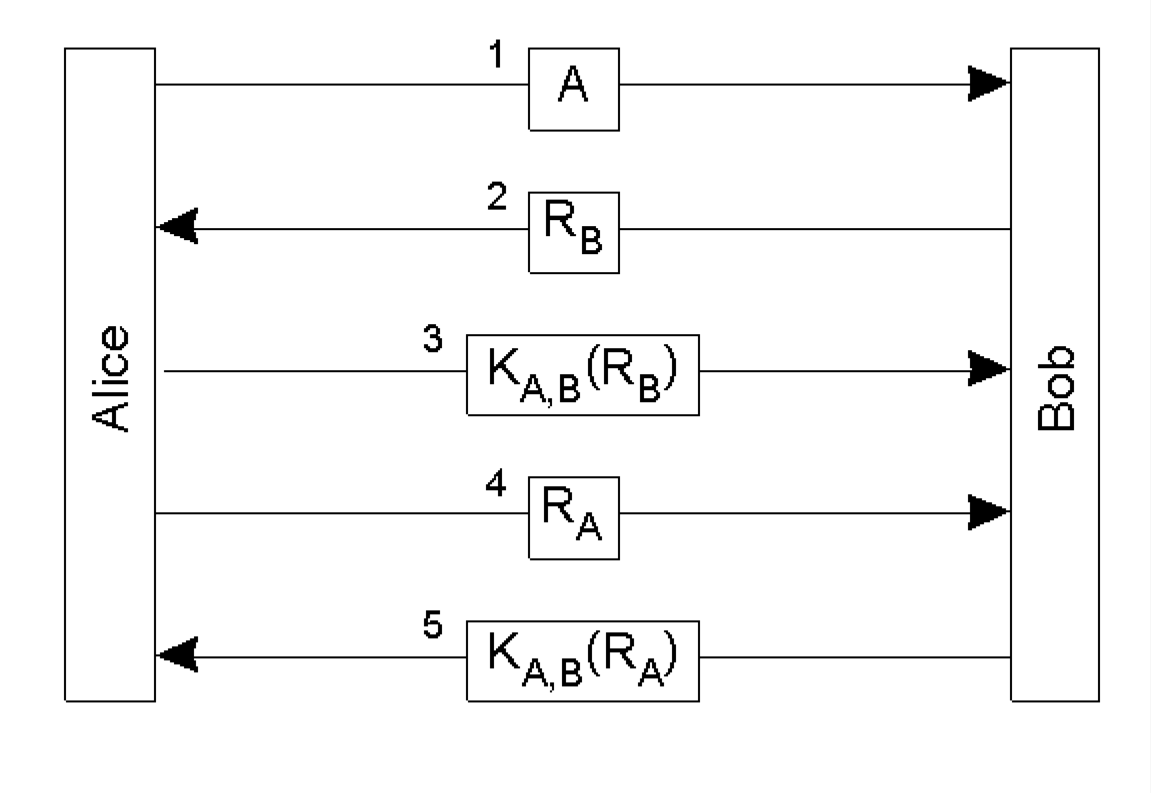
Hash Functions : MD5 (2)



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

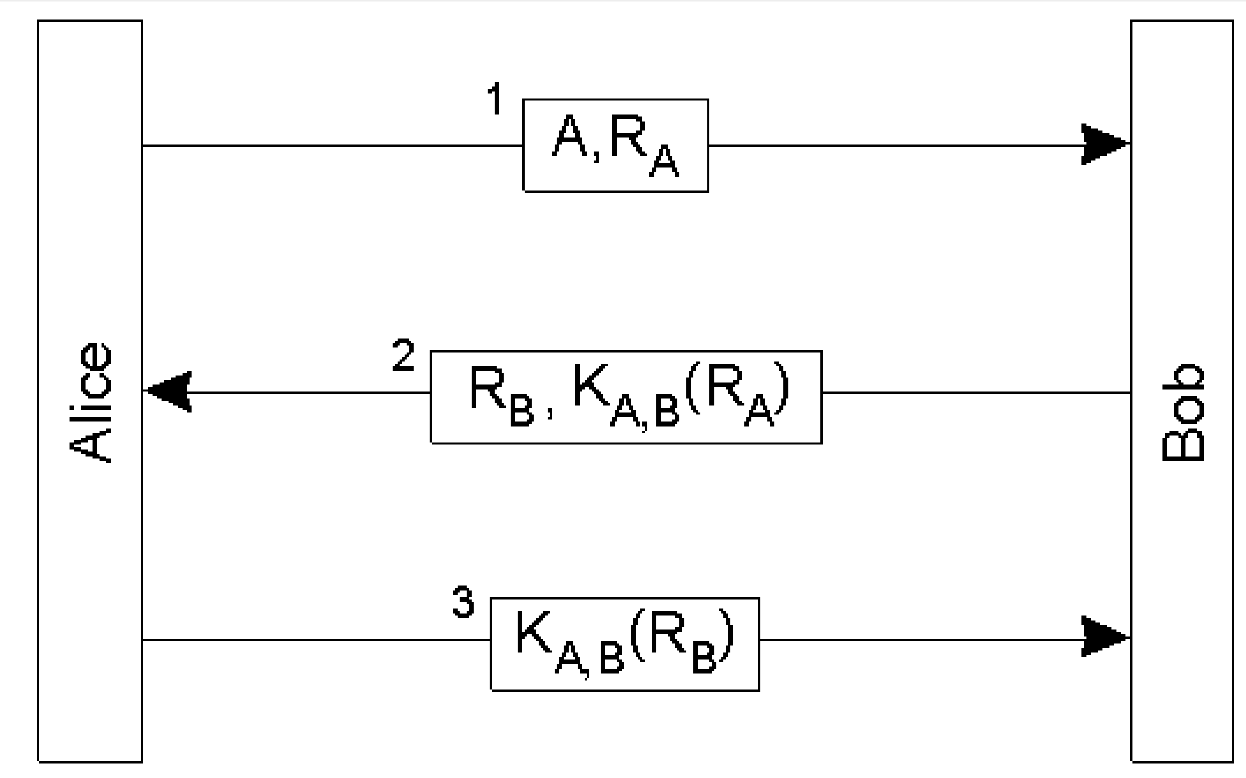
Authentication (1)

- Autl

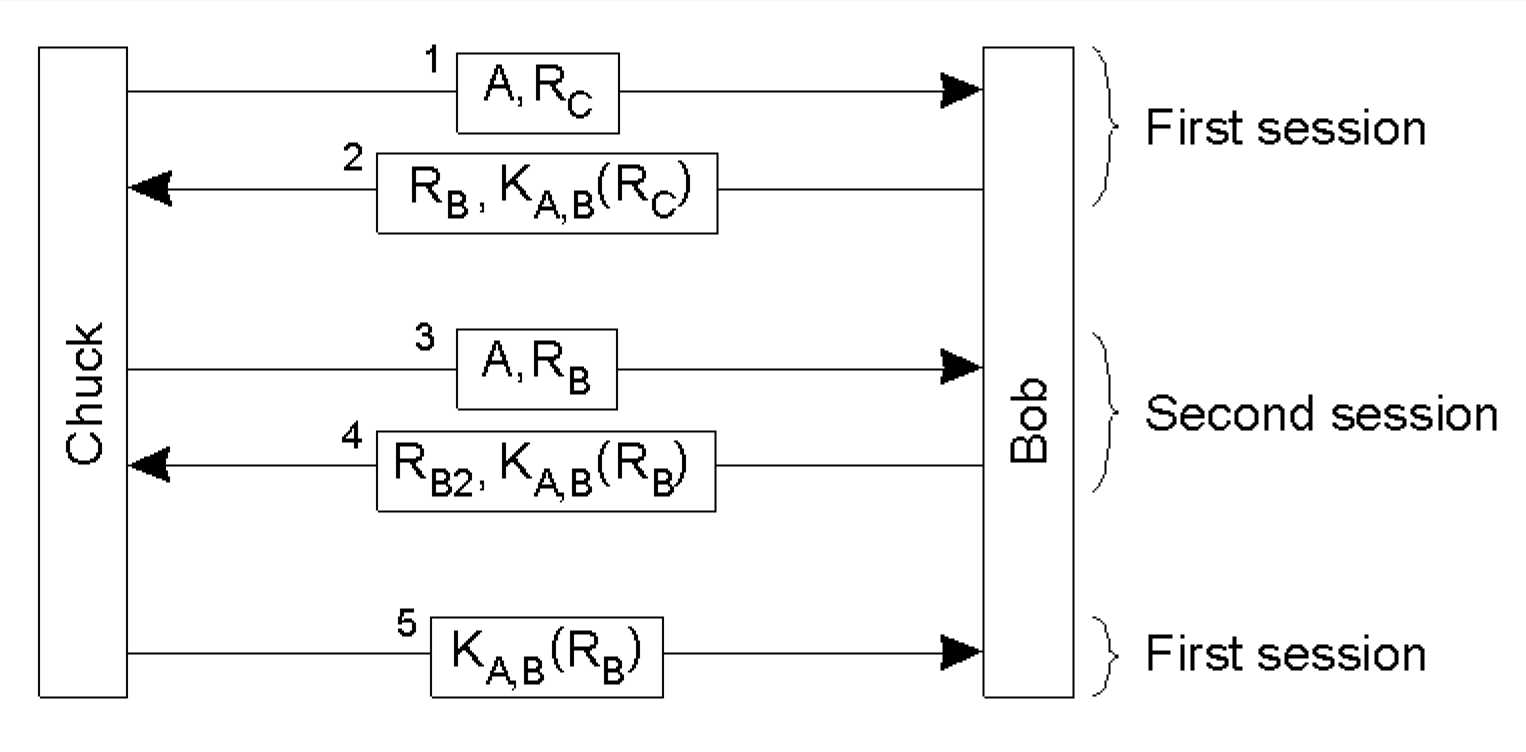


Authentication (2)

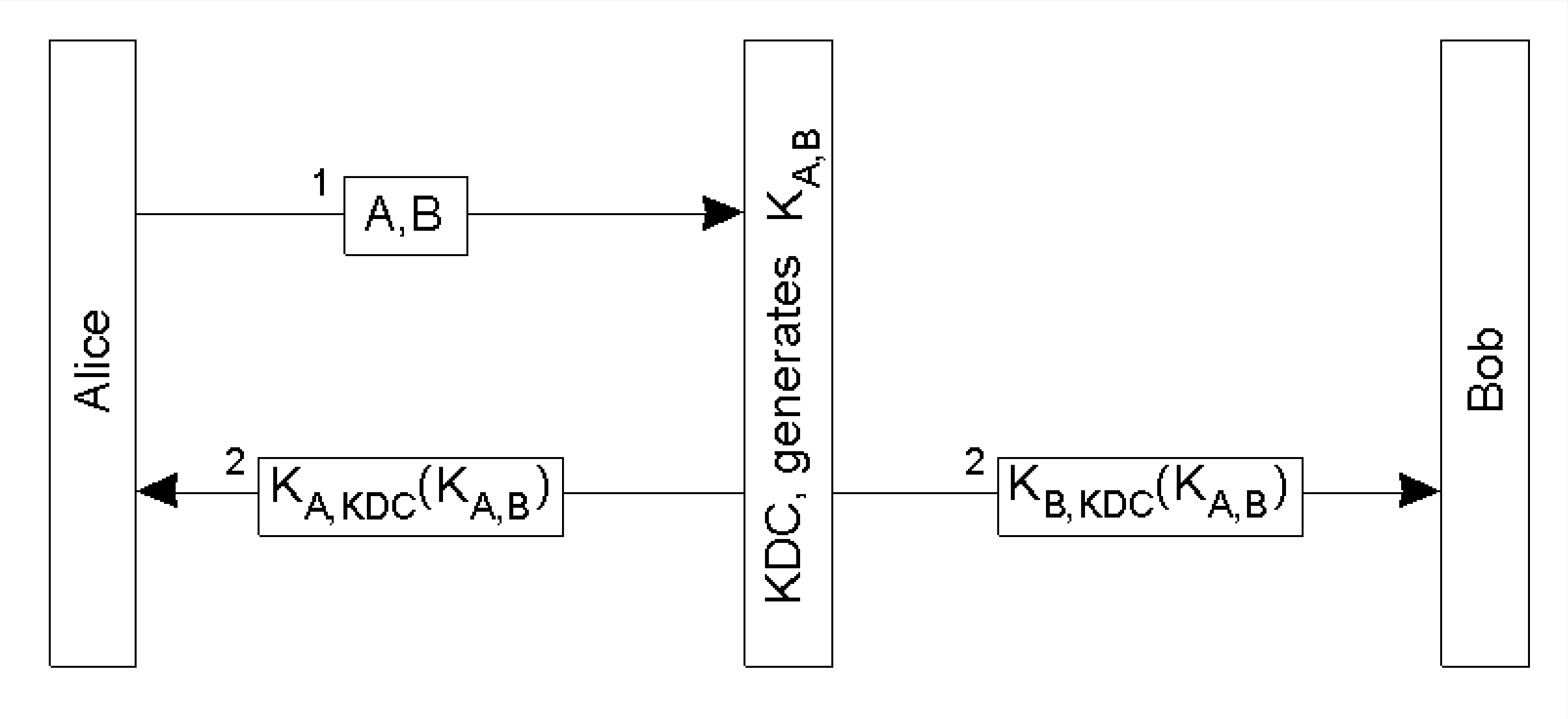
- Au instead of
  fiv



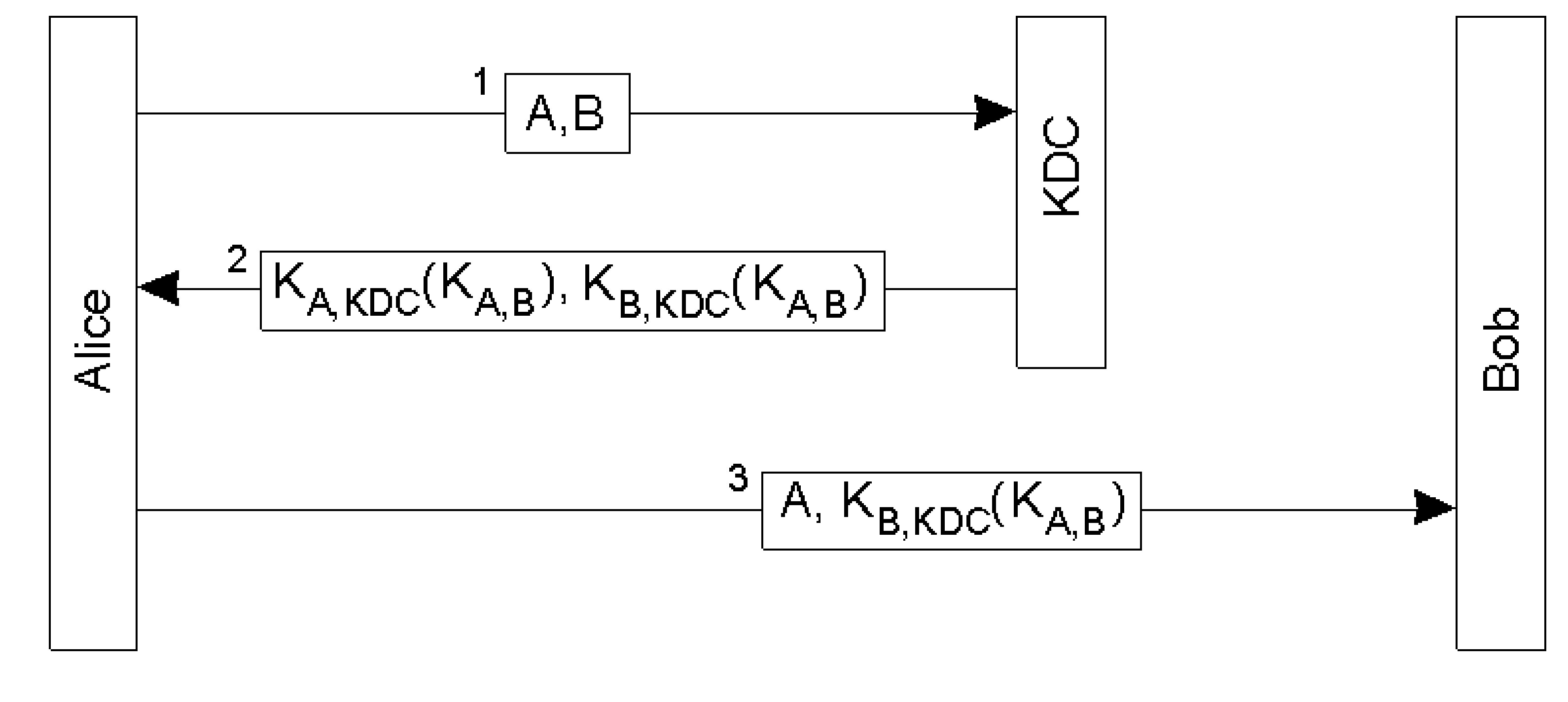
Authentication (3)



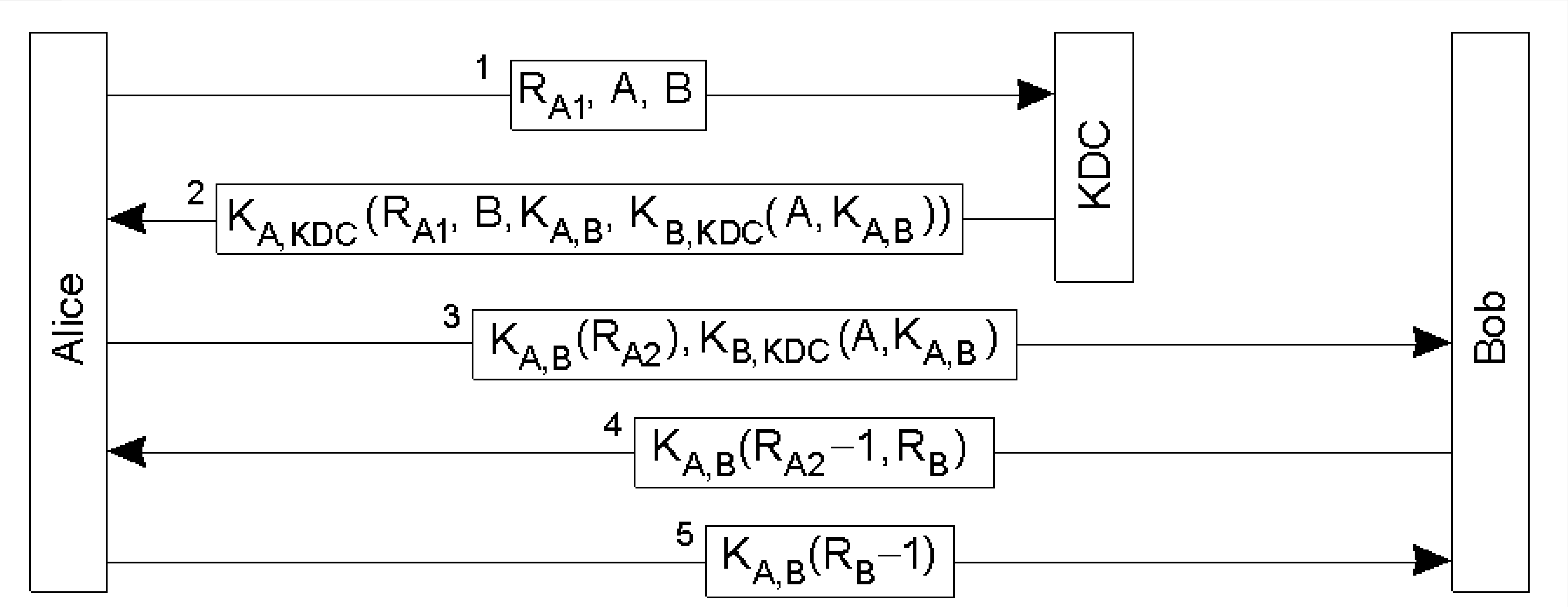
Authentication Using a Key Distribution Center (1)



Authentication Using a Key Distribution Center (2)



Authentication Using a Key Distribution Center (3)



1 R_{A1}, A, B

2 $K_{A,KDC}(R_{A1}, B, K_{A,B}, K_{B,KDC}(A, K_{A,B}))$

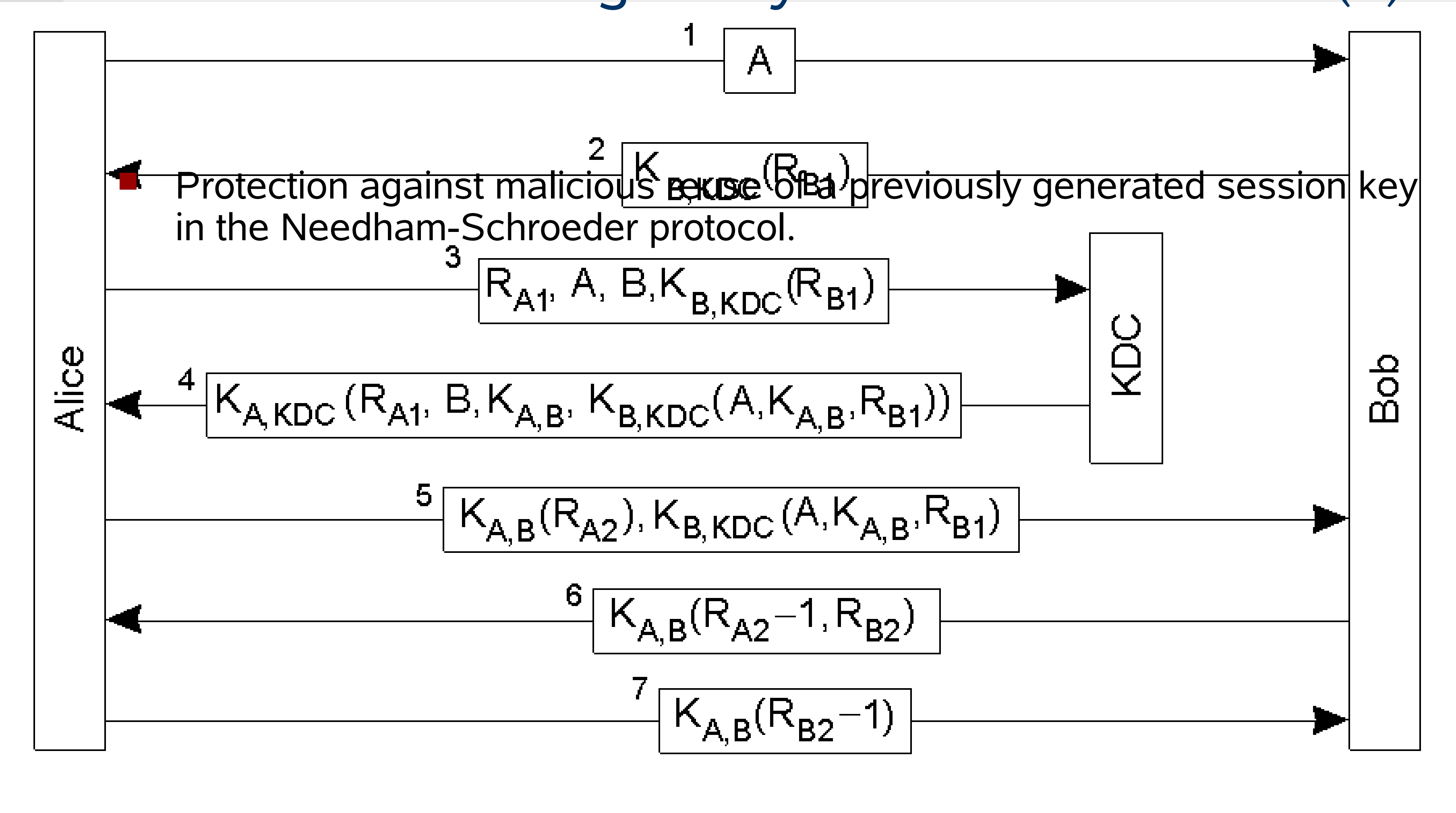
3 $K_{A,B}(R_{A2}), K_{B,KDC}(A, K_{A,B})$

4 $K_{A,B}(R_{A2}-1, R_B)$

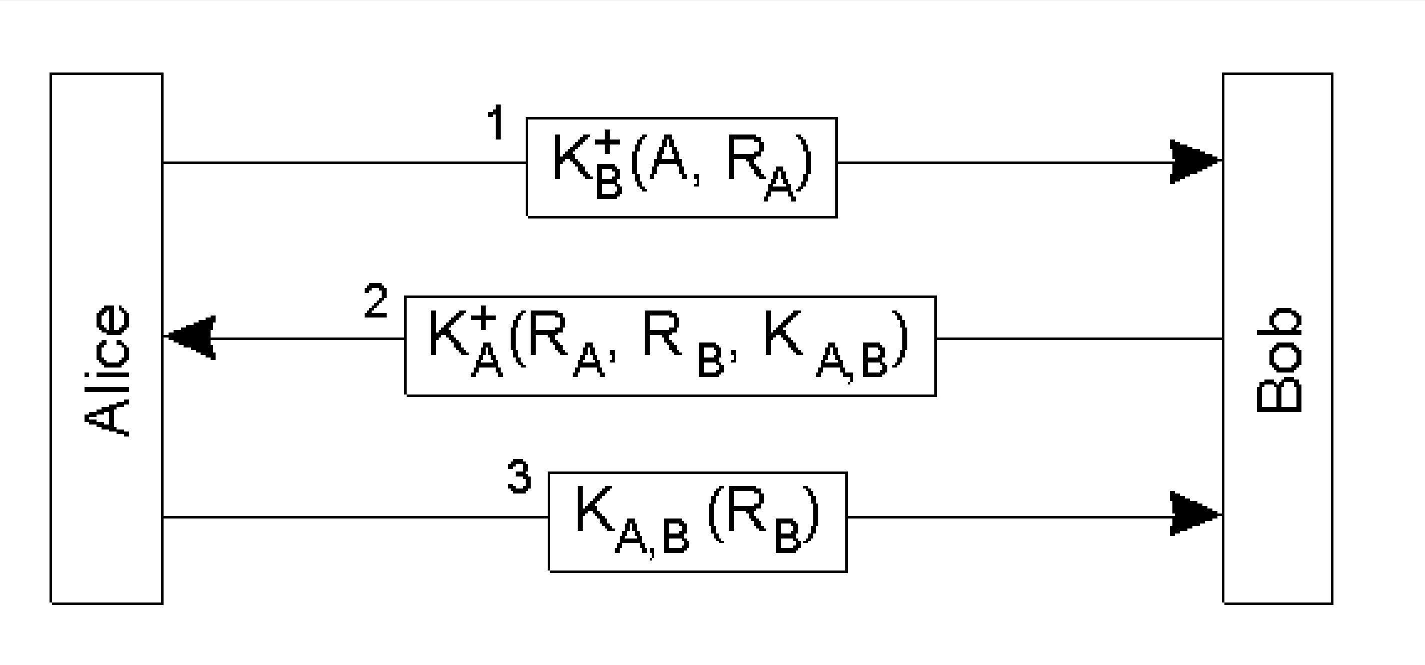
5 $K_{A,B}(R_B-1)$

Authentication Using a Key Distribution Center (4)

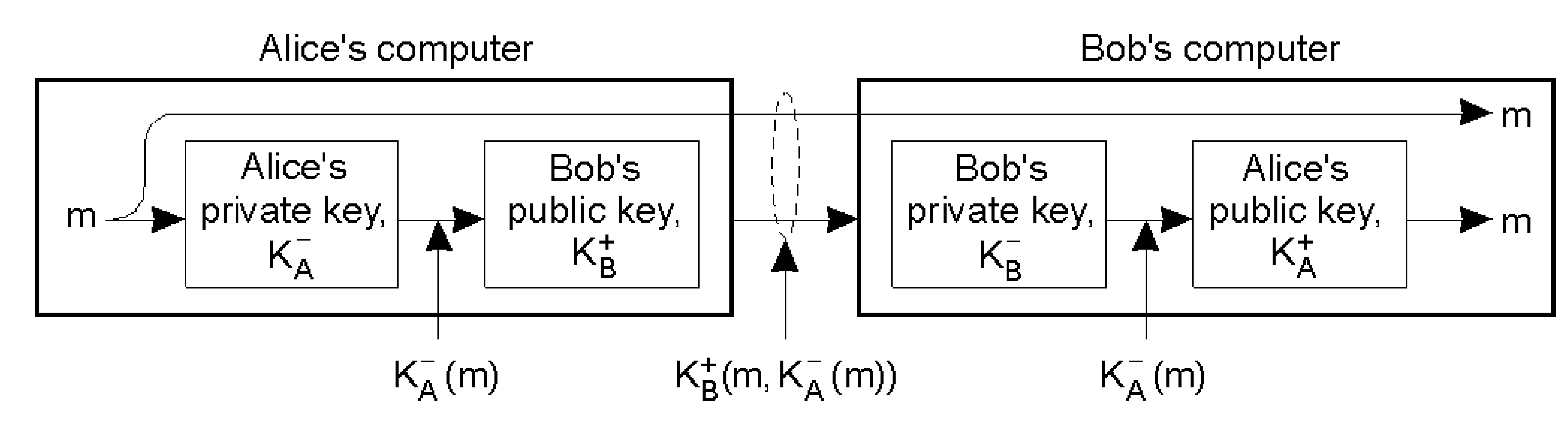
- Protection against malicious reuse of a previously generated session key in the Needham-Schroeder protocol.


Alice
KDC
Bob
1
A
2
$K_{B,KDC}(R_{B1})$
3
$R_{A1}, A, B, K_{B,KDC}(R_{B1})$
4
$K_{A,KDC}(R_{A1}, B, K_{A,B}, K_{B,KDC}(A, K_{A,B}, R_{B1}))$
5
$K_{A,B}(R_{A2}), K_{B,KDC}(A, K_{A,B}, R_{B1})$
6
$K_{A,B}(R_{A2}-1, R_{B2})$
7
$K_{A,B}(R_{B2}-1)$

Authentication Using Public-Key Cryptography

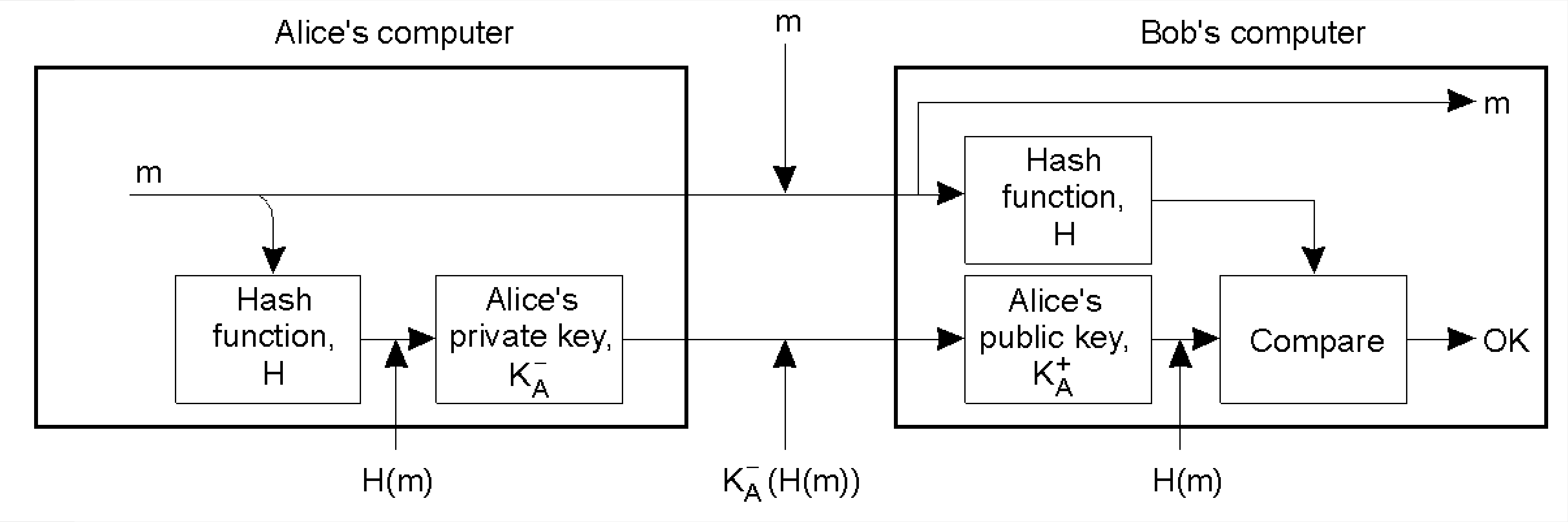
- 

Digital Signatures (1)


Alice's computer
Bob's computer
m
Alice's private key, K_A^-
Bob's public key, K_B^+
Bob's private key, K_B^-
Alice's public key, K_A^+
m
m
$K_A^-(m)$
$K_B^+(m, K_A^-(m))$
$K_A^-(m)$

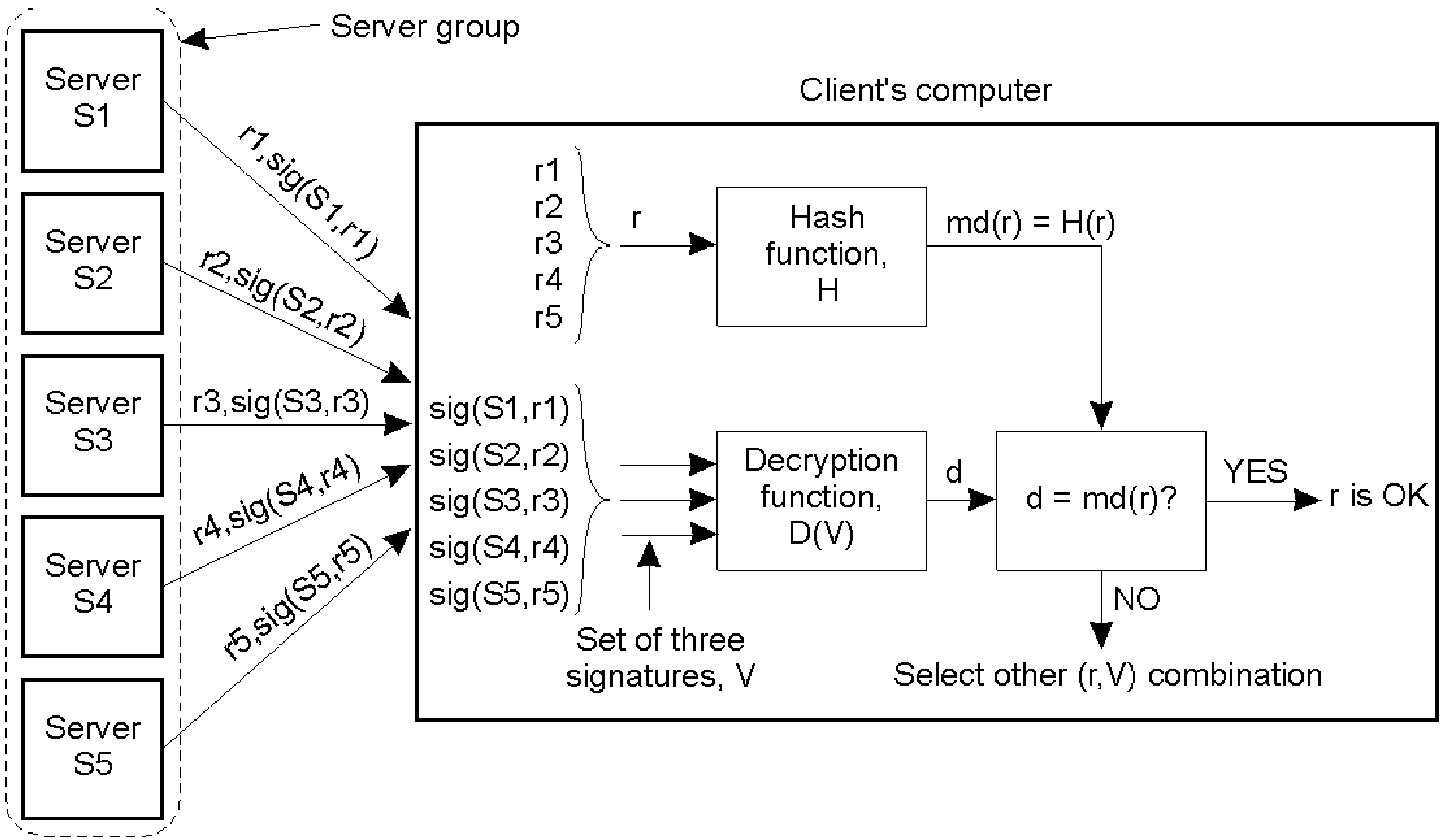
- Digital signing a message using public-key cryptography.

Digital Signatures (2)

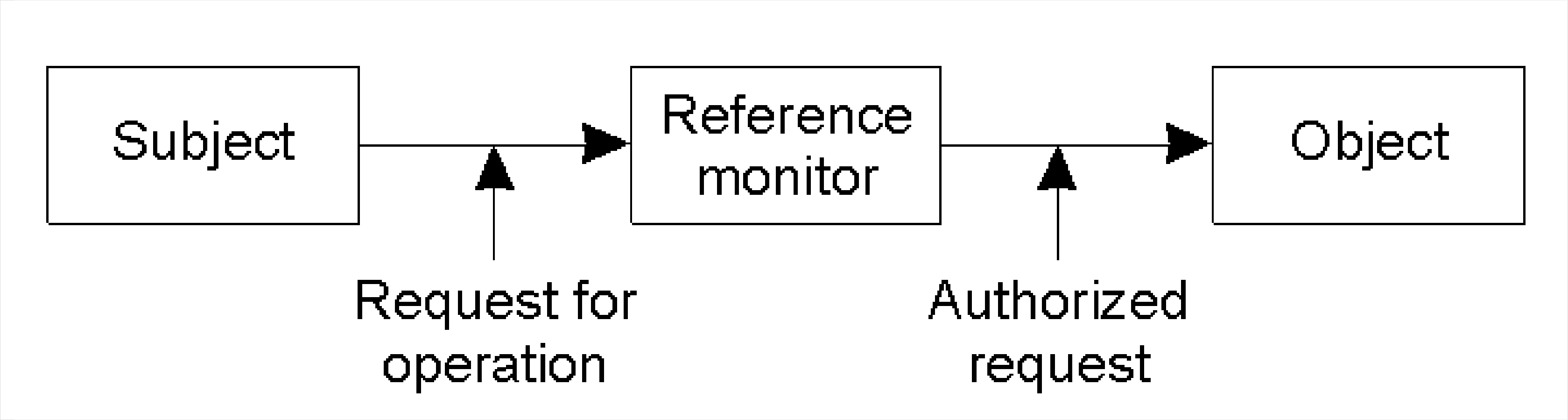


- Digitally signing a message using a message digest.

Secure Replicated Services



General Issues in Access Control



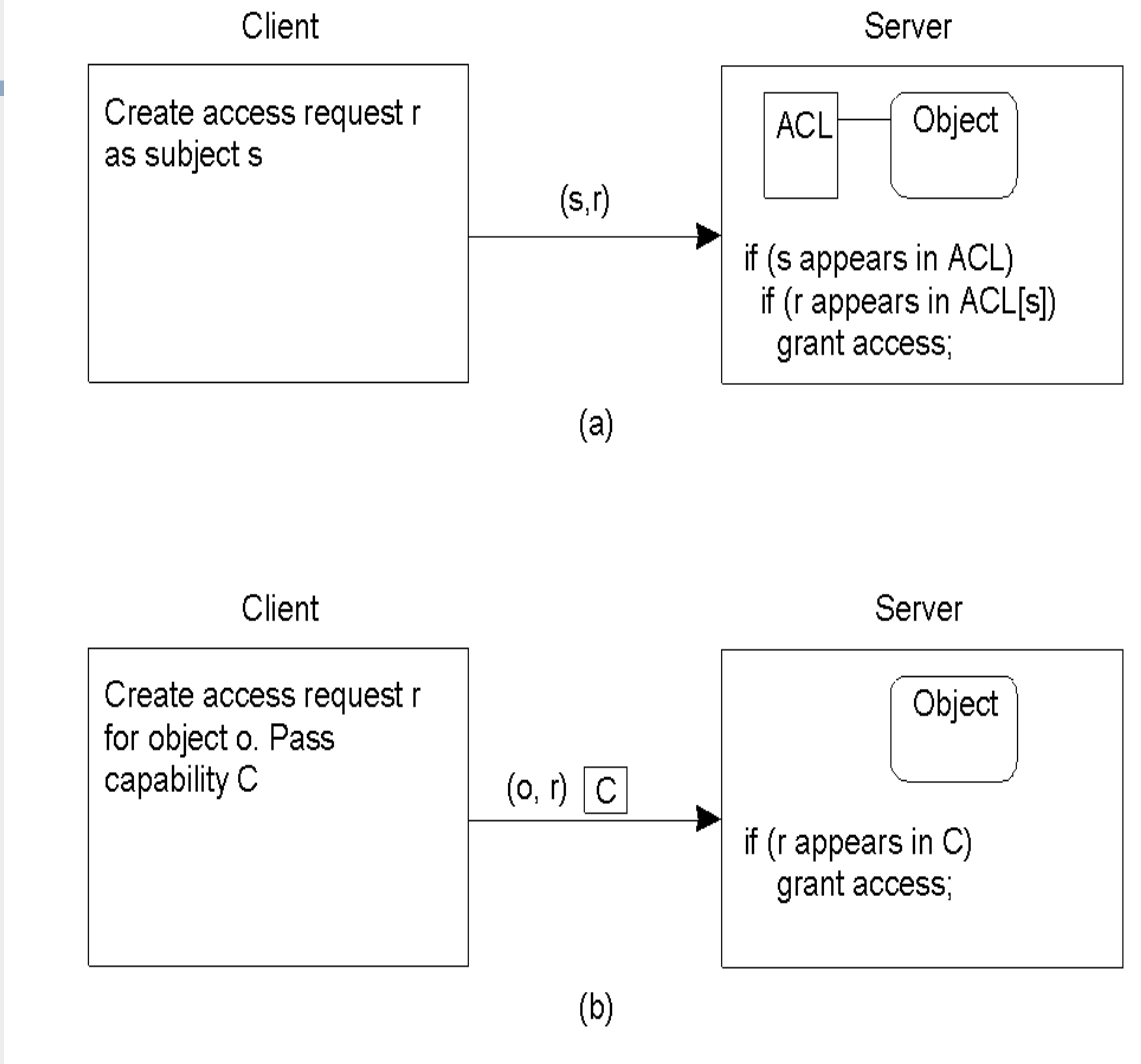
- General model of controlling access to objects.

Access Control Matrix

- Comparison between ACLs and capabilities for protecting objects.

a) Using an ACL

b) Using capabilities.



Client

Create access request r as subject s

(s,r)

Server

ACL

Object

```
if (s appears in ACL)
  if (r appears in ACL[s])
    grant access;
```

(a)

Client

Create access request r for object o. Pass capability C

(o, r) C

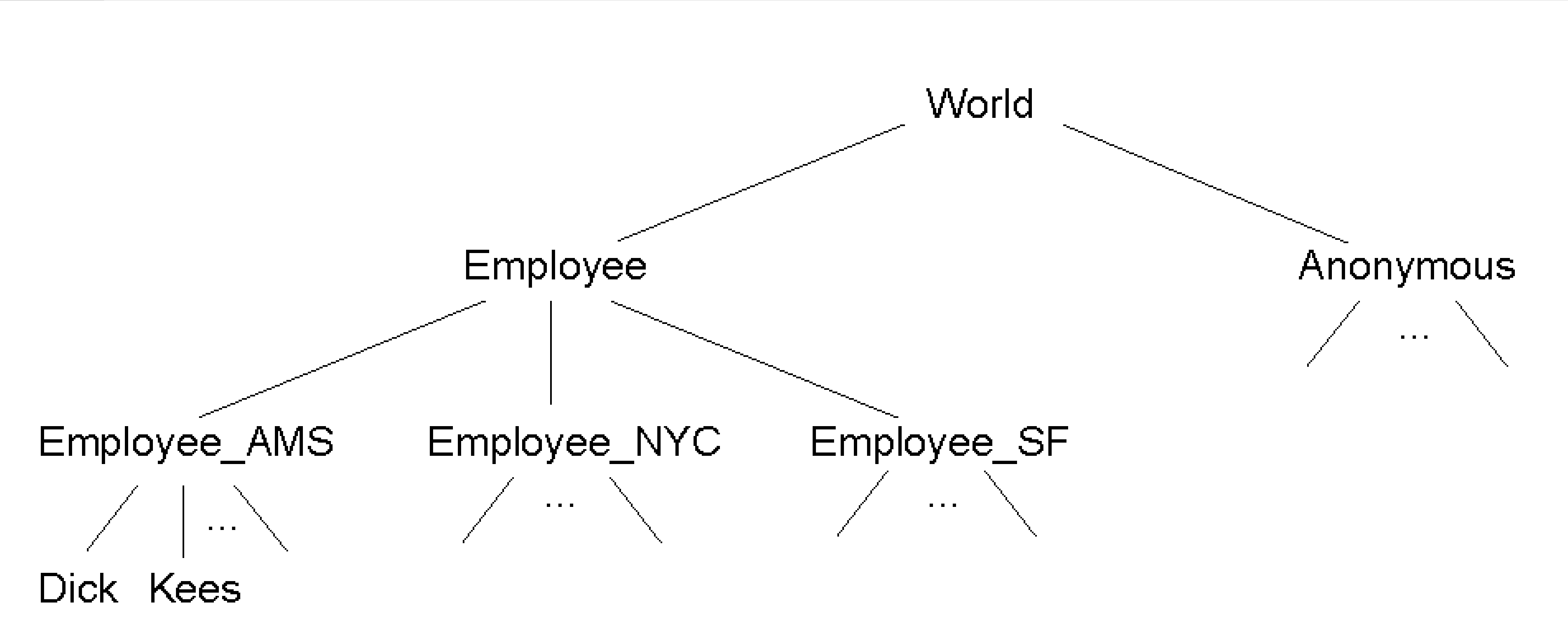
Server

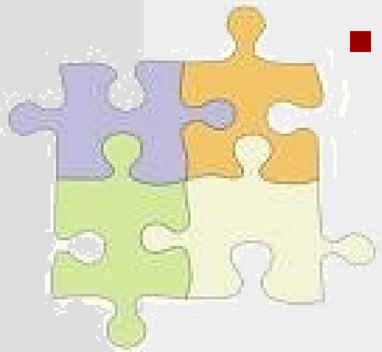
Object

```
if (r appears in C)
  grant access;
```

(b)

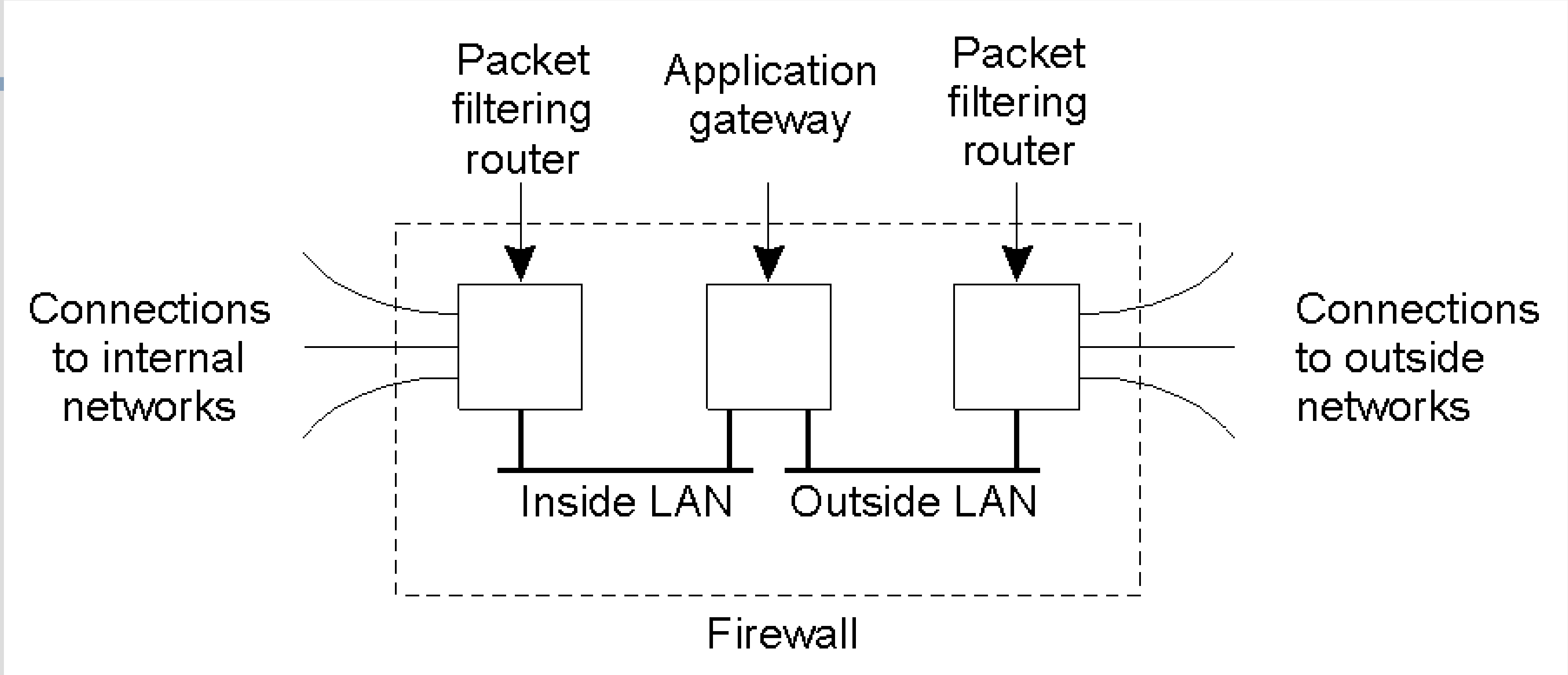
Protection Domains



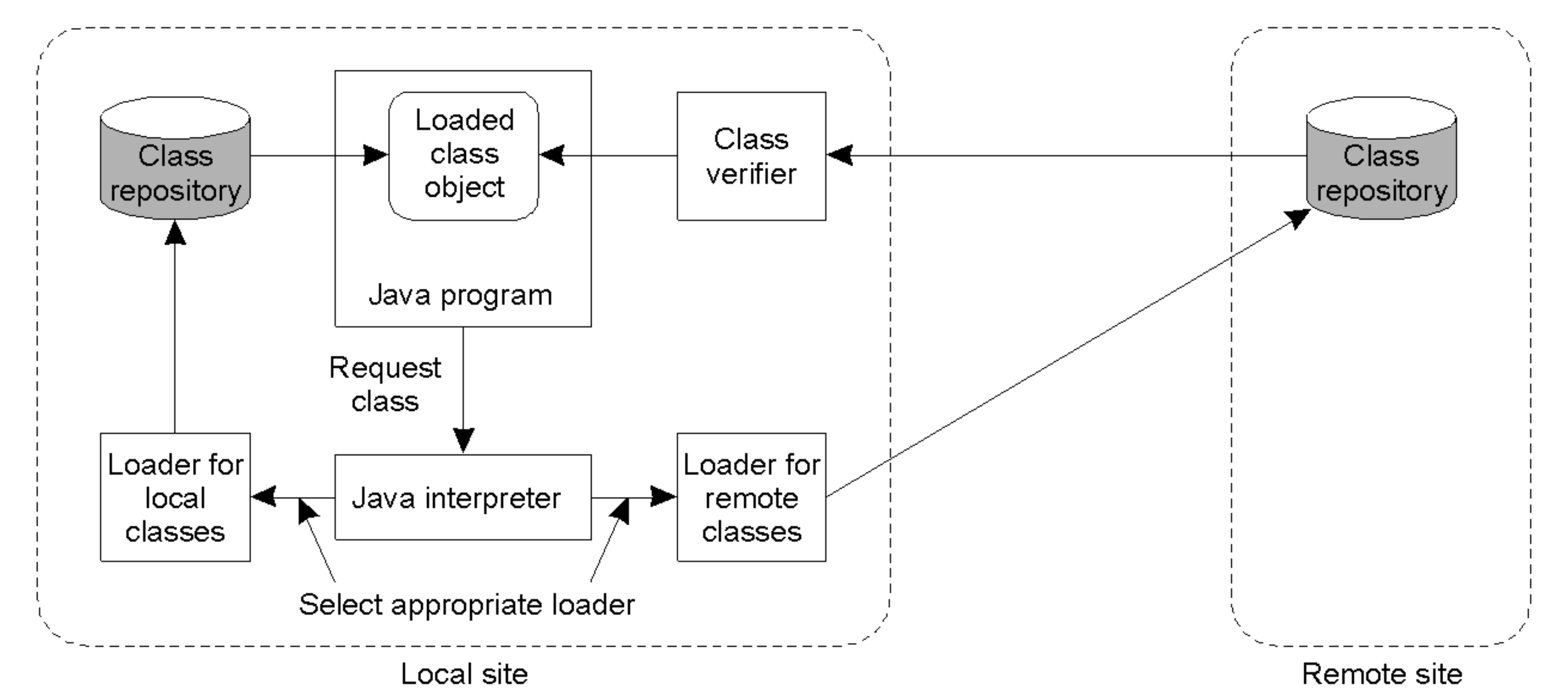


- The hierarchical organization of protection domains as groups of users.

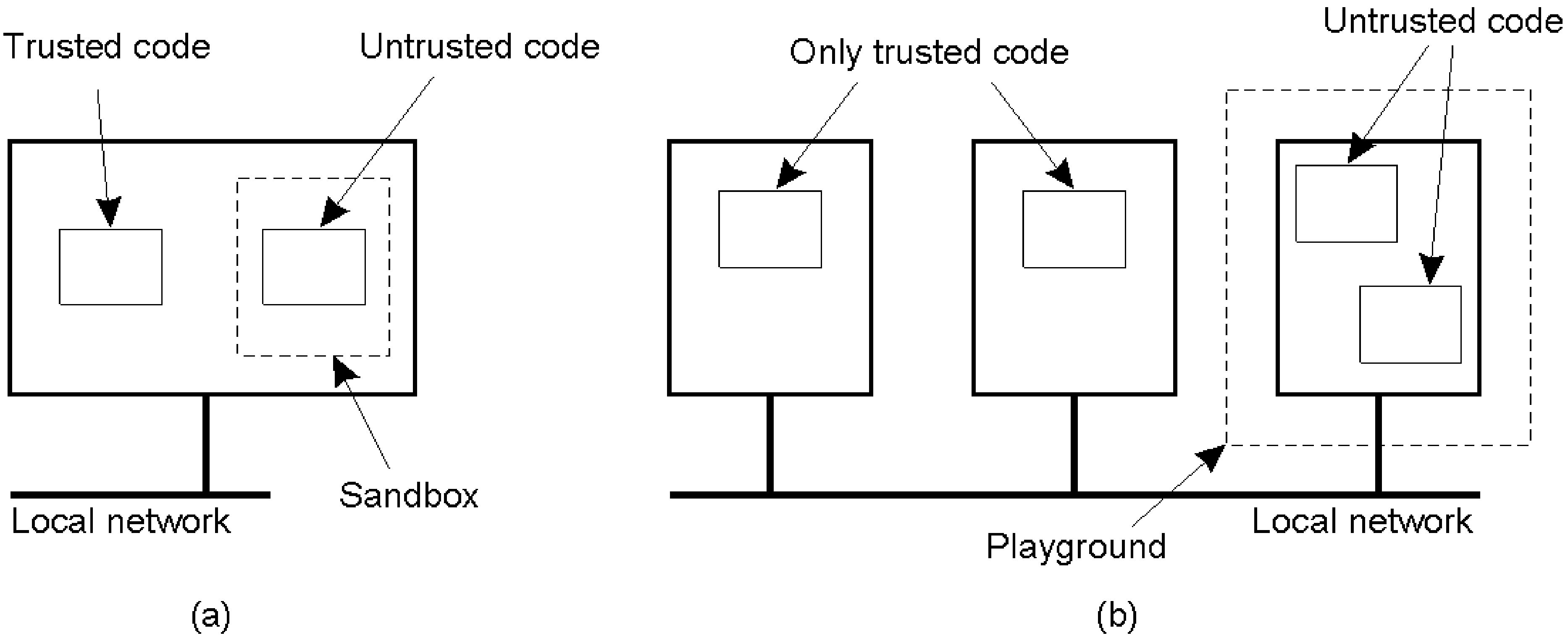
Firewalls


Packet filtering router
Application gateway
Packet filtering router
Connections to internal networks
Connections to outside networks
Inside LAN
Outside LAN
Firewall

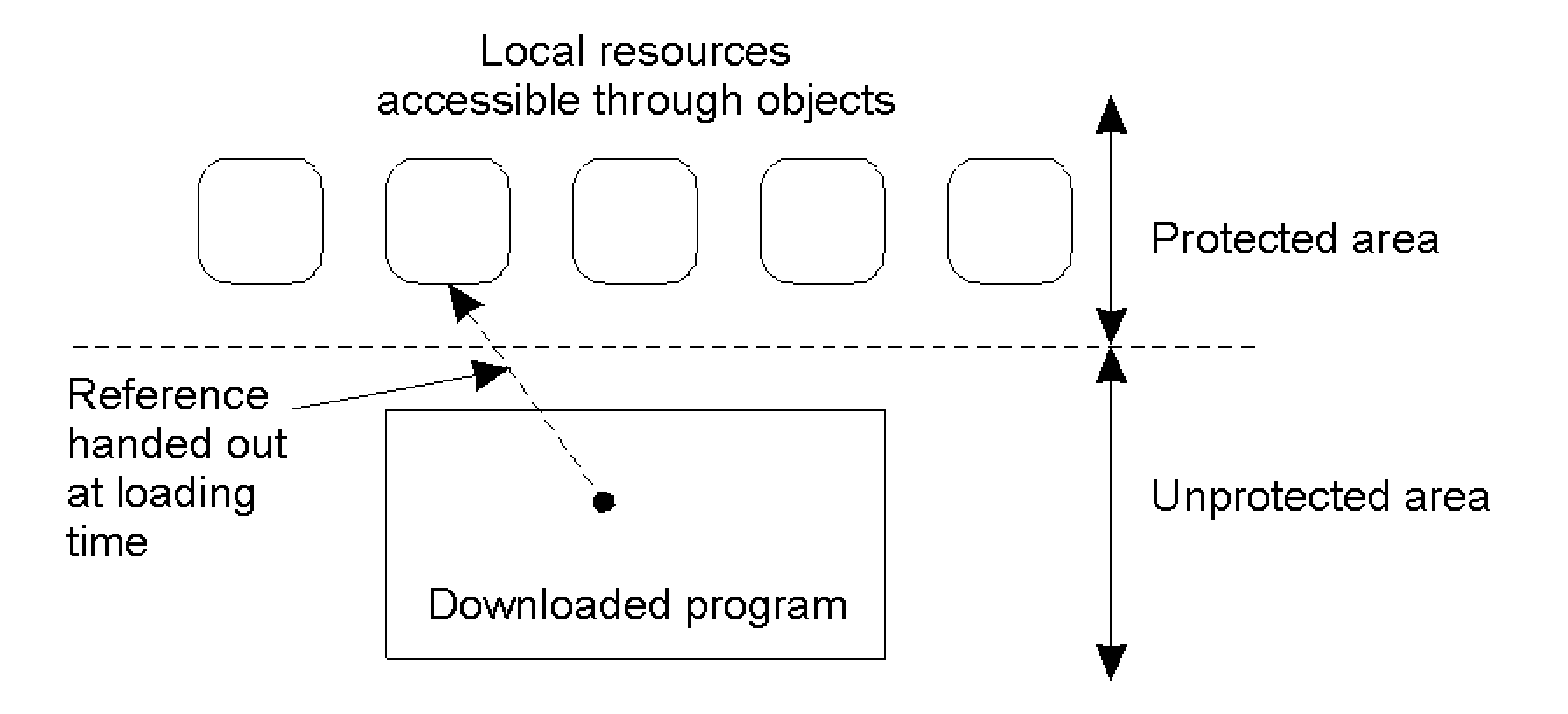
Protecting the Target (1)



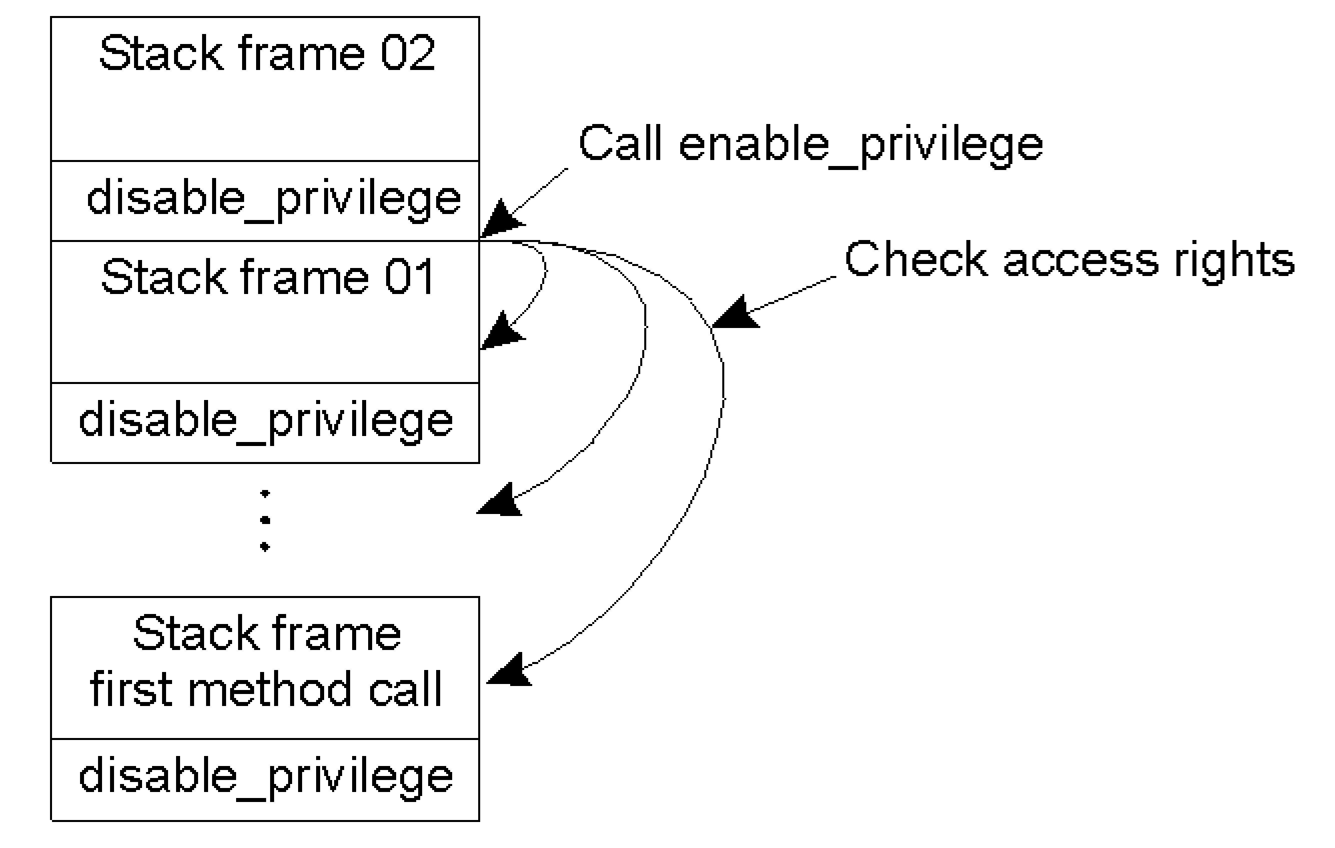
Protecting the Target (2)



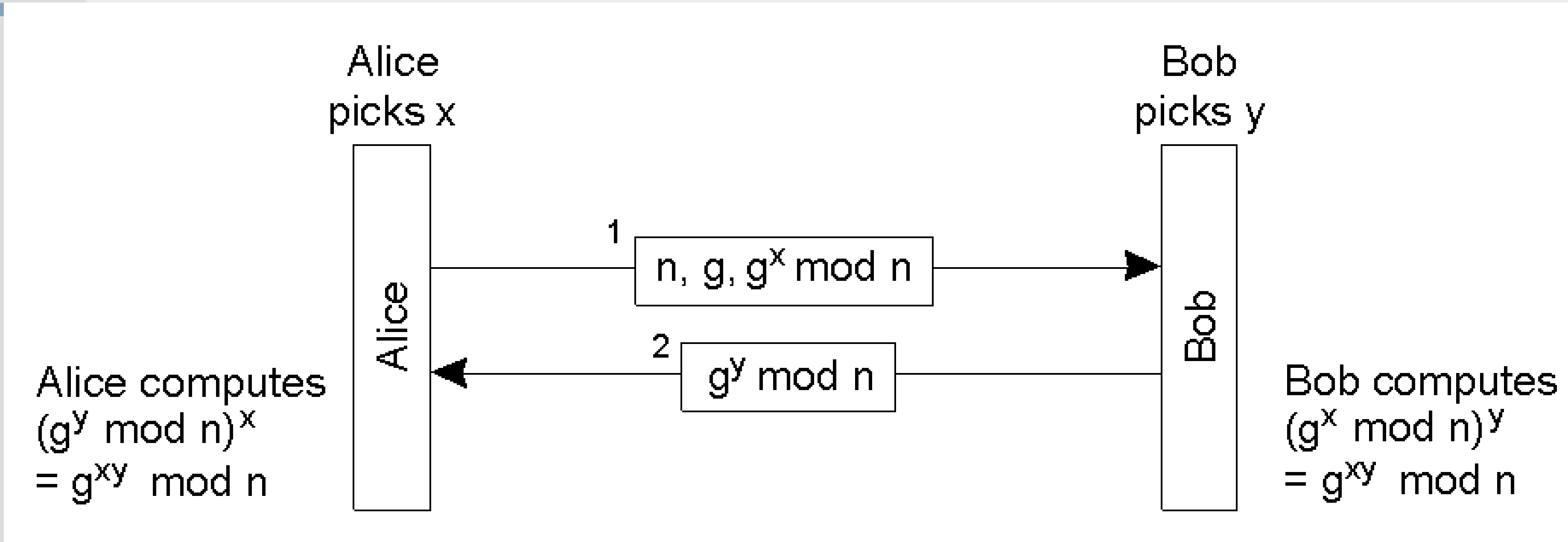
Protecting the Target (3)


Local resources accessible through objects
Protected area
Reference handed out at loading time
Unprotected area
Downloaded program

Protecting the Target (4)



Key Establishment



Alice picks x

Bob picks y

Alice

Bob

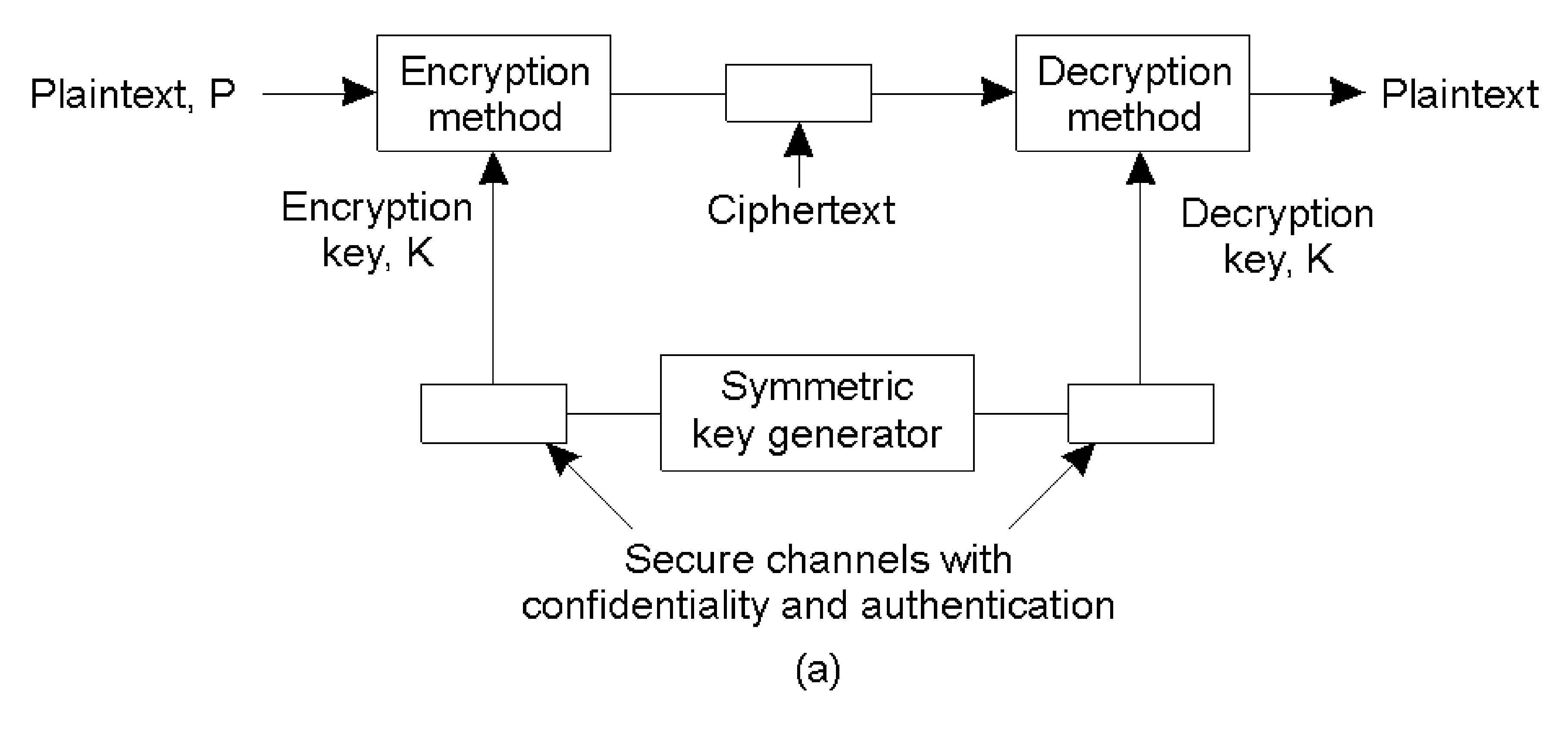
1 n, g, g^x mod n

2 g^y mod n

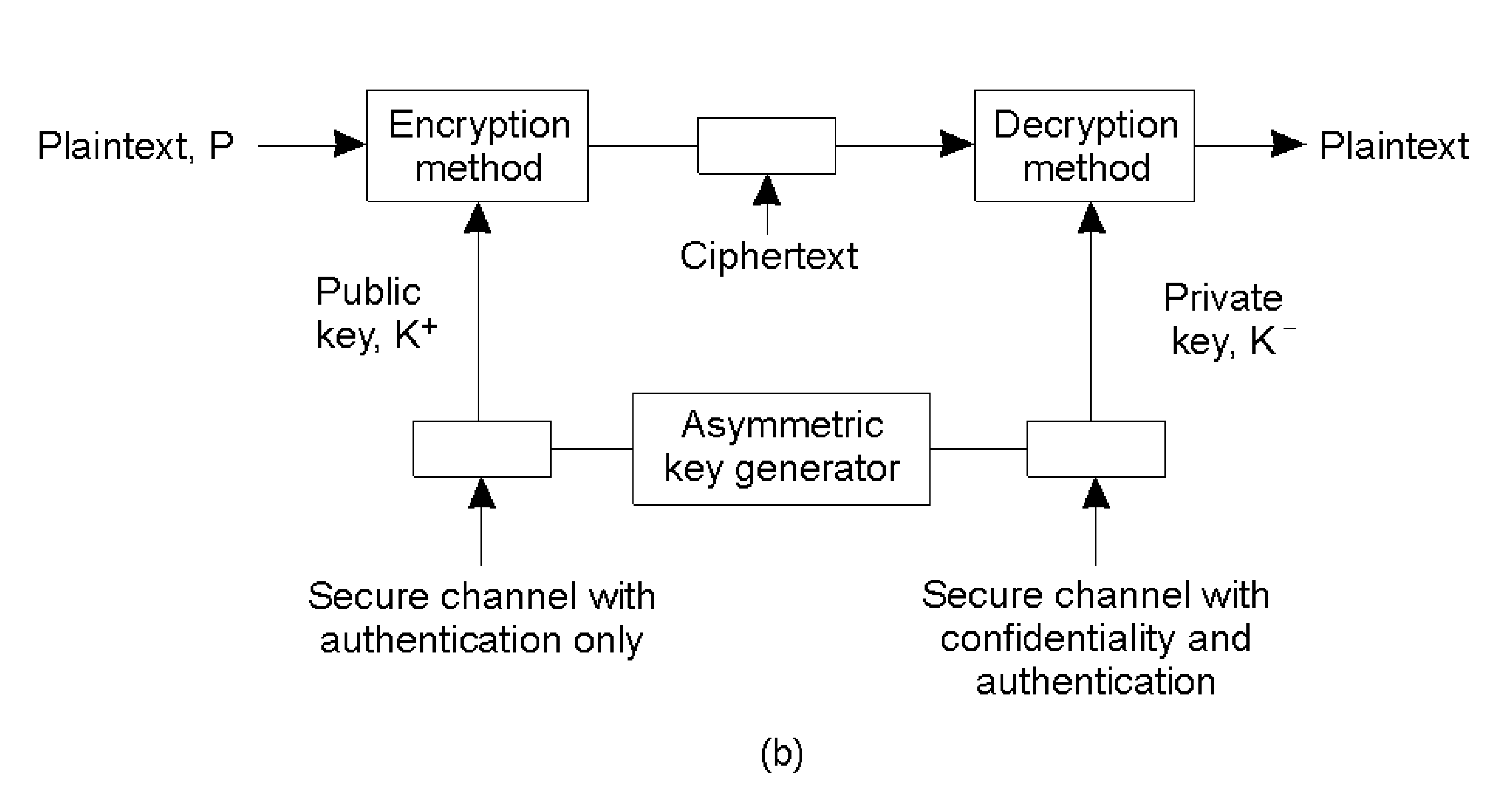
Alice computes
(g^y mod n)^x
= g^{xy} mod n

Bob computes
(g^x mod n)^y
= g^{xy} mod n

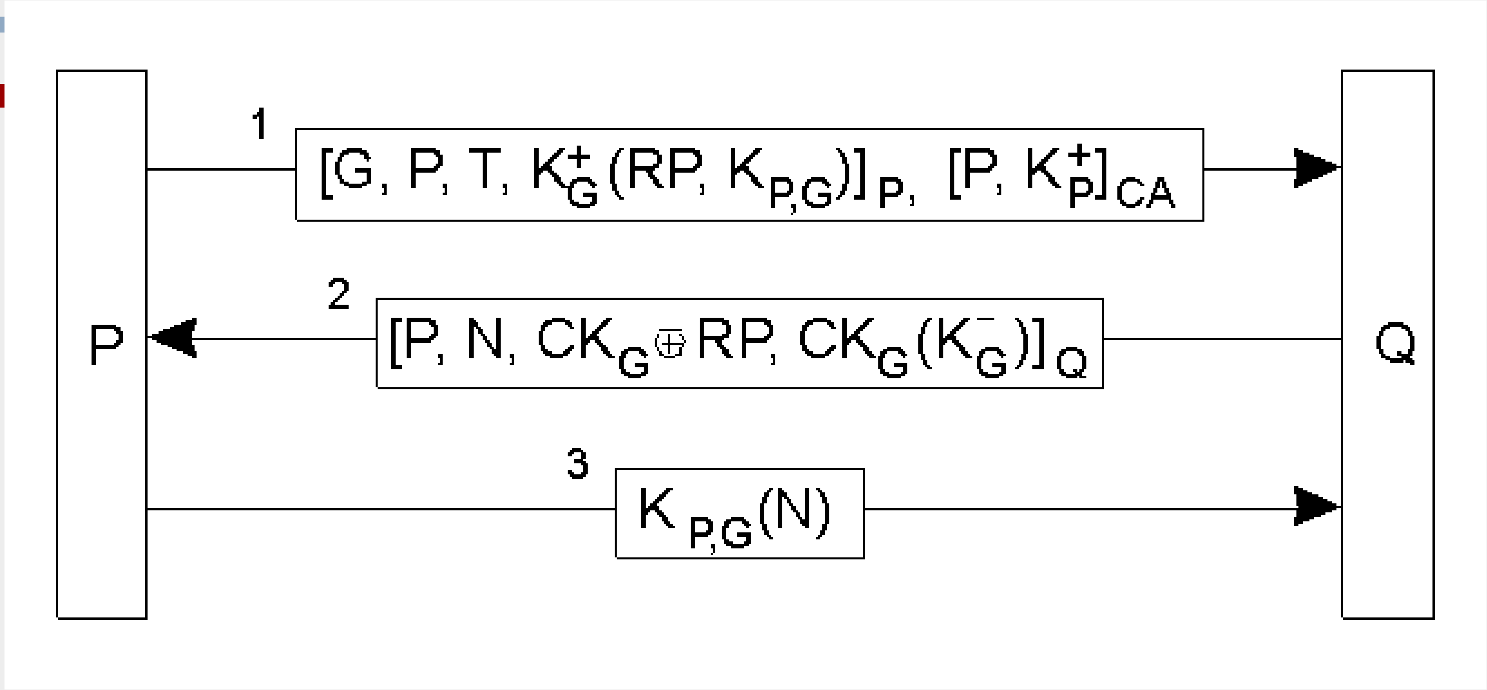
Key Distribution (1)



Key Distribution (2)



Secure Group Management

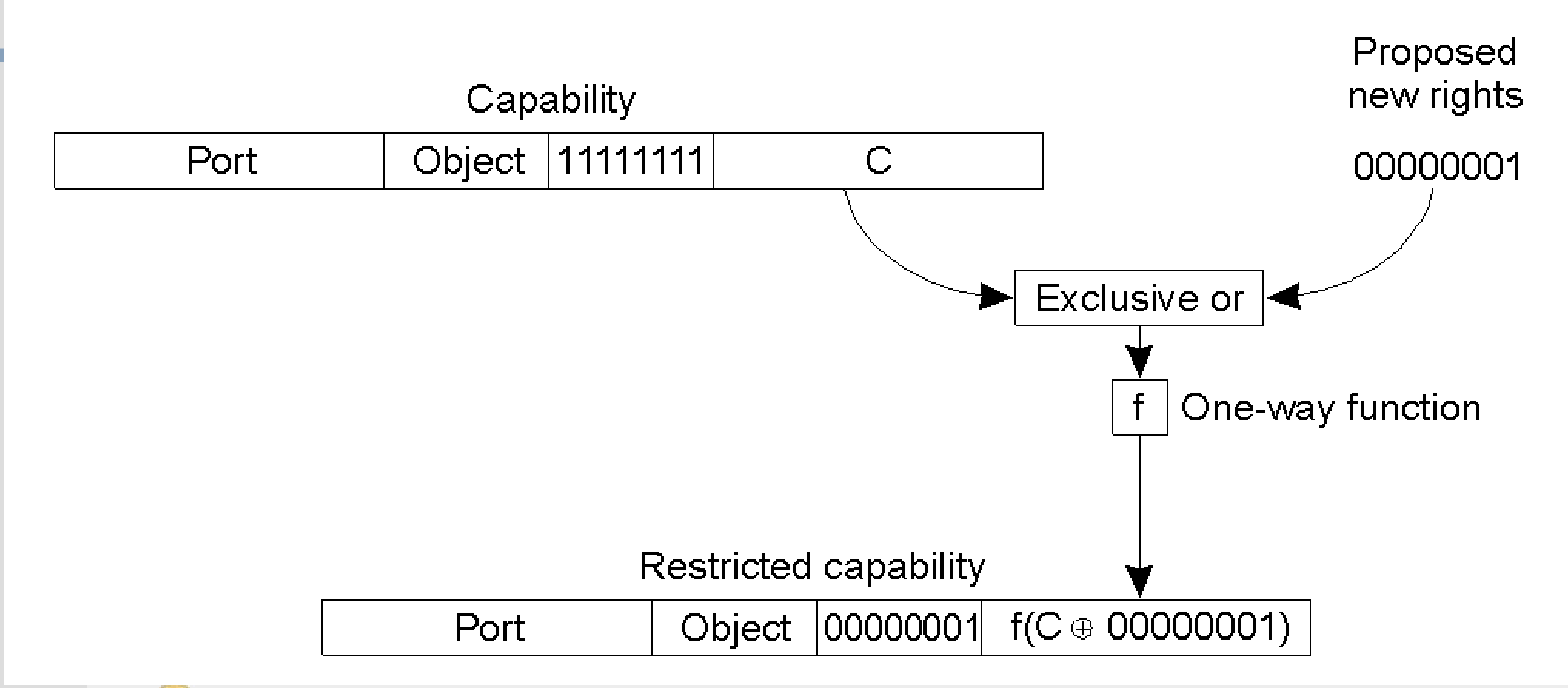

P
Q
1
$[G, P, T, K_G^+(RP, K_{P,G})]_P, \ [P, K_P^+]_{CA}$
2
$[P, N, CK_G \oplus RP, CK_G(K_G^-)]_Q$
3
$K_{P,G}(N)$

Capabilities and Attribute Certificates (1)

48 bits	24 bits	8 bits	48 bits
Server port	Object	Rights	Check

- A capability in Amoeba.

Capabilities and Attribute Certificates (2)



Capability

Port	Object	11111111	C

Proposed new rights

00000001

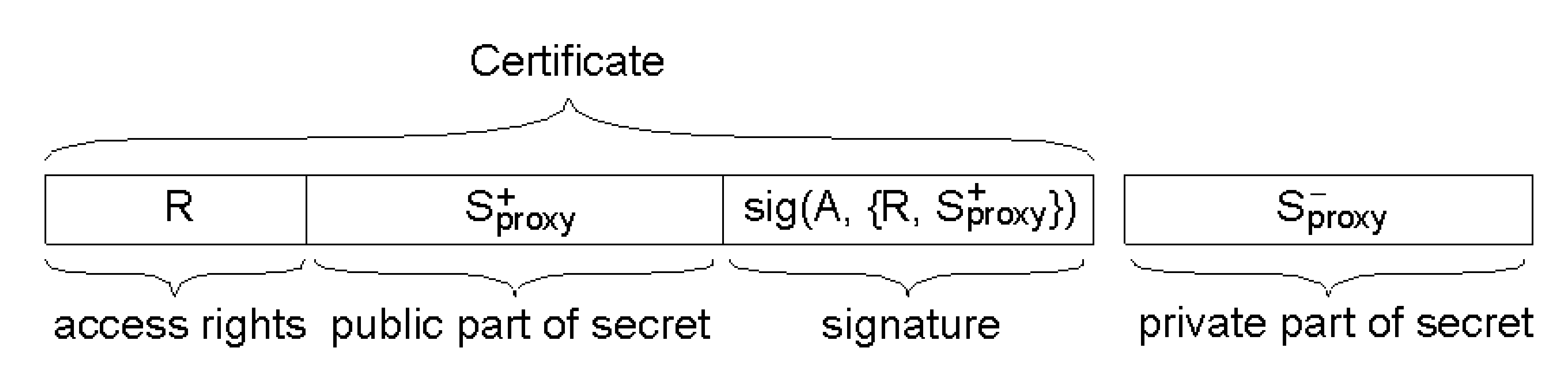
Exclusive or

f One-way function

Restricted capability

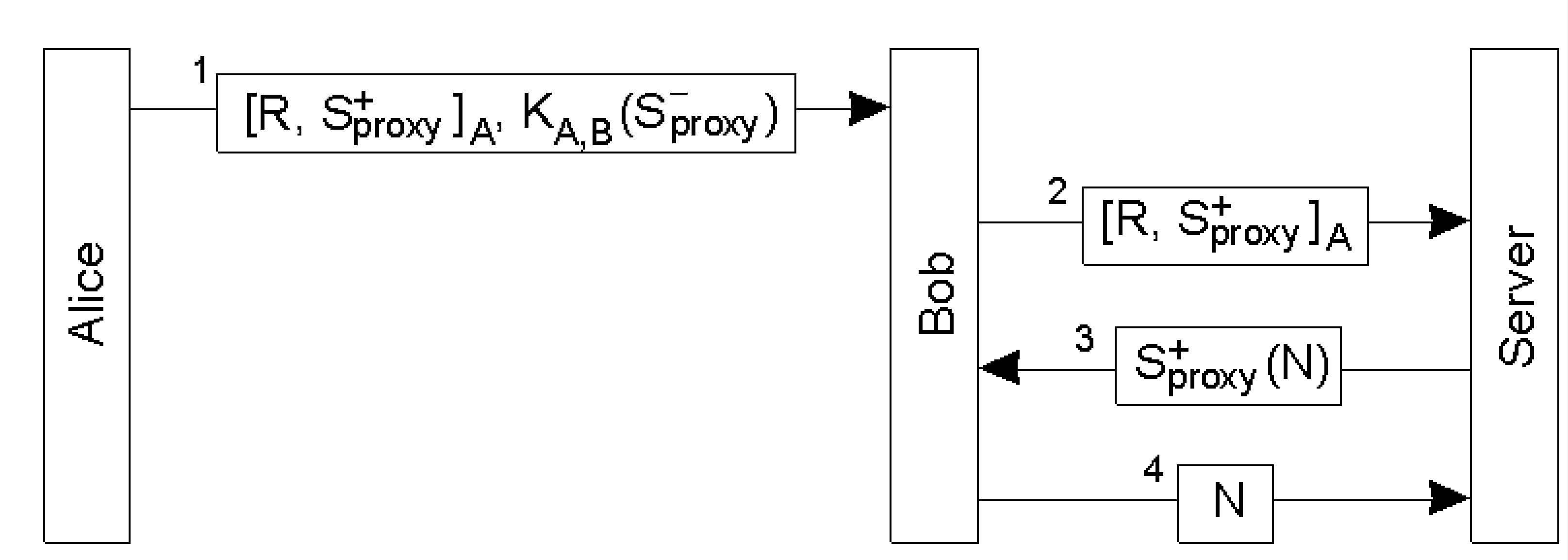
Port	Object	00000001	f(C ⊕ 00000001)

Delegation (1)

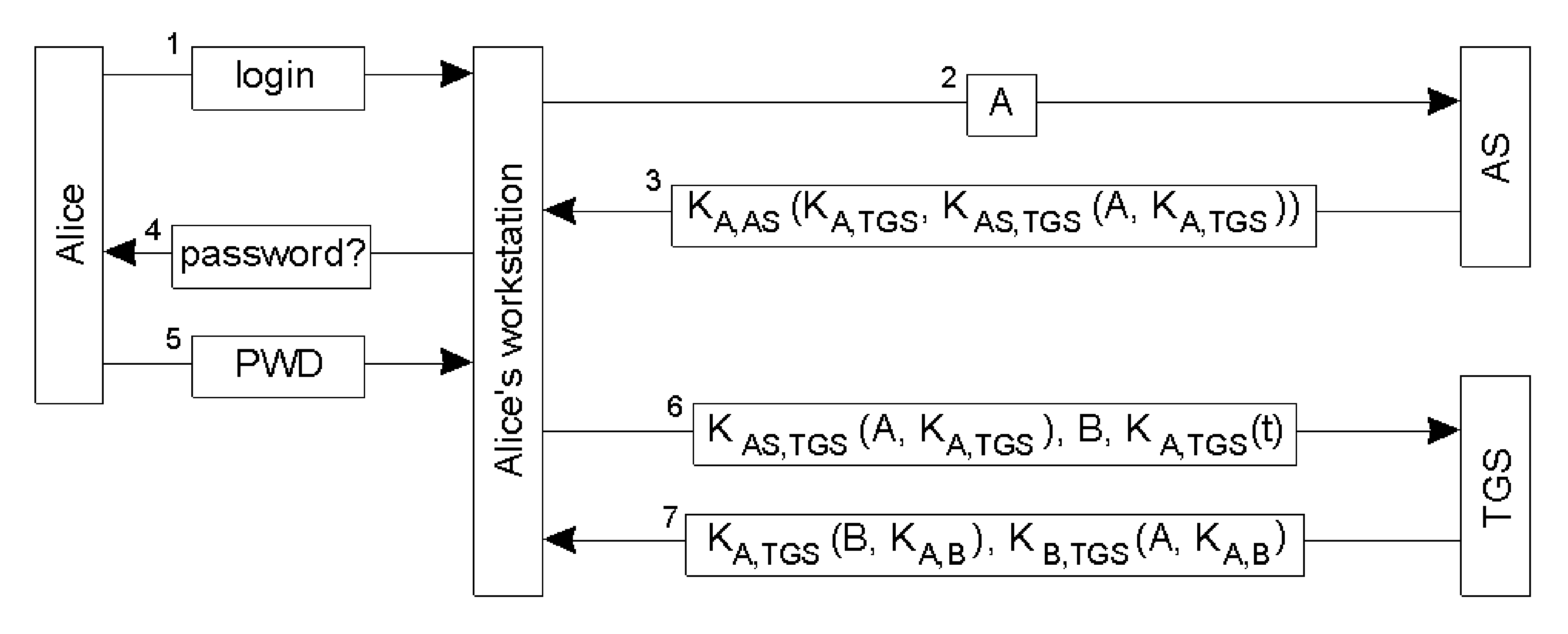


- The general structure of a proxy as used for delegation.

Delegation (2)

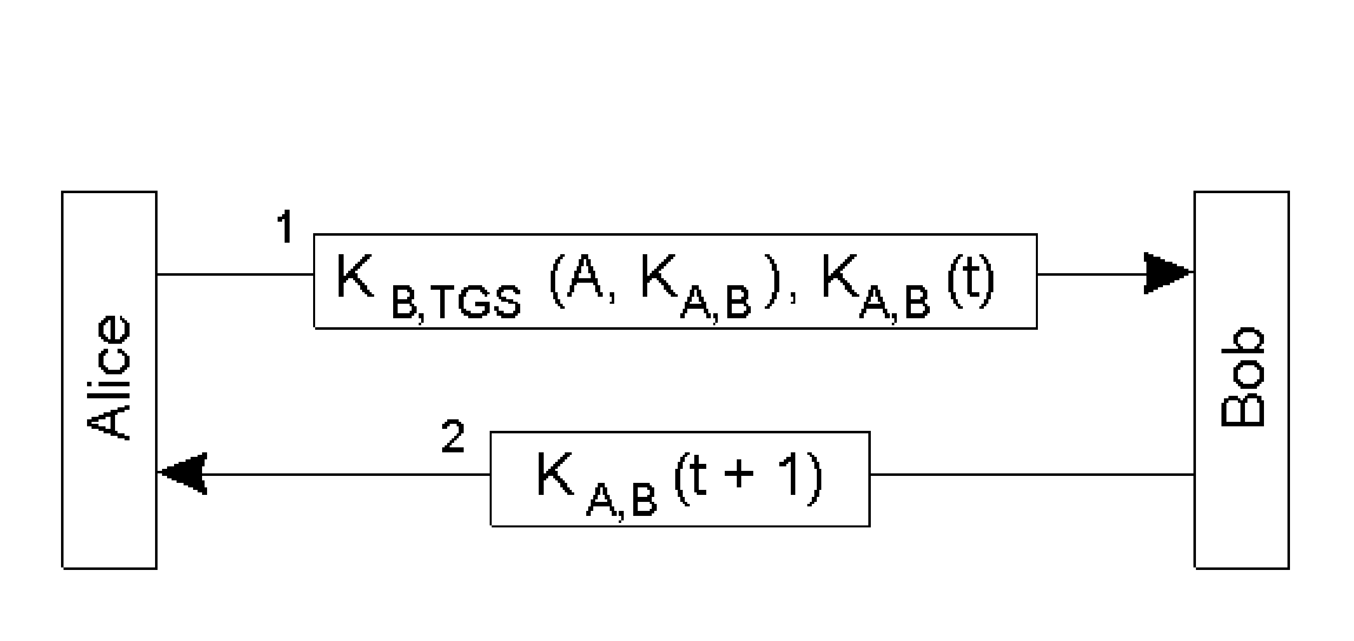


Example: Kerberos (1)

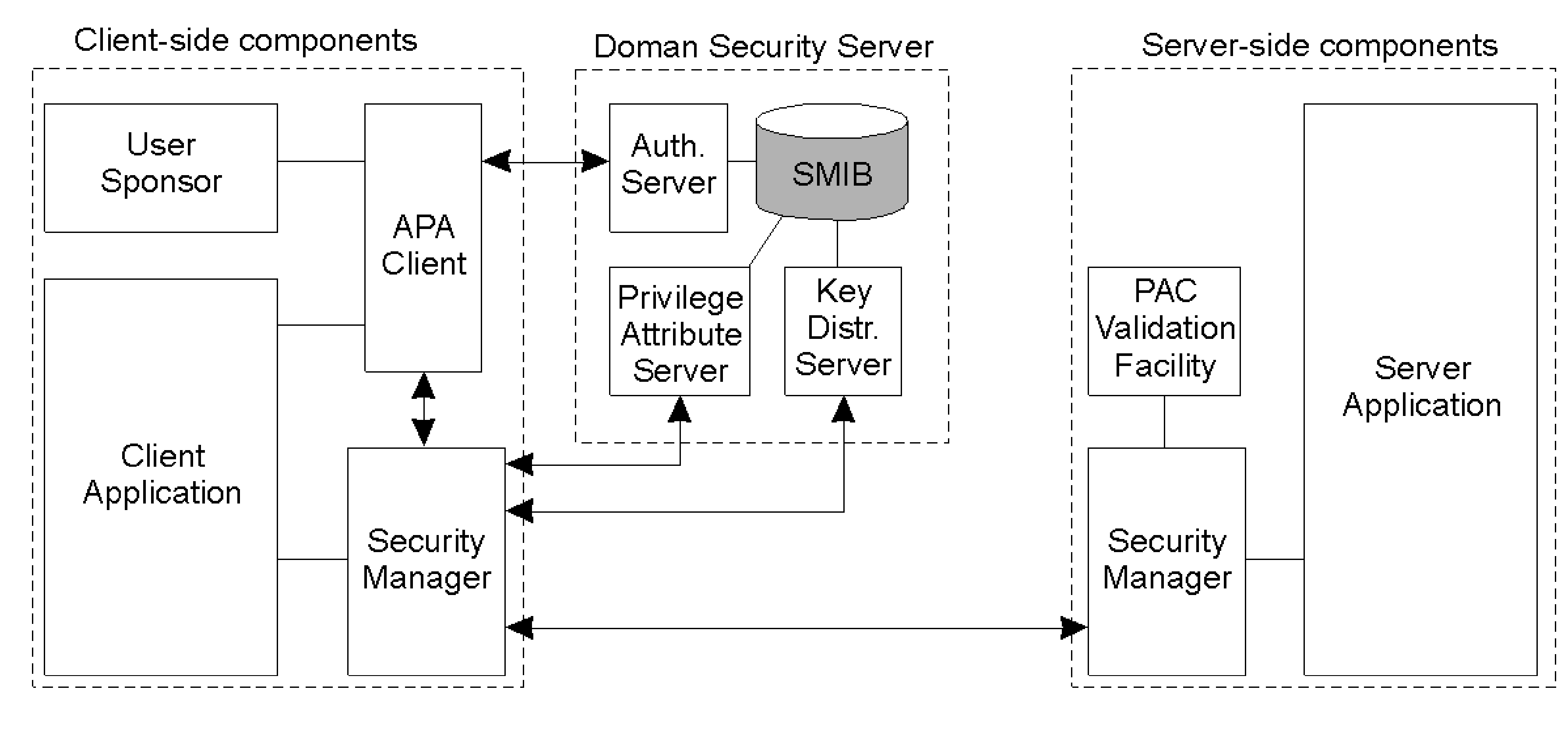

Alice
Alice's workstation
AS
TGS
1
login
2
A
3
$K_{A,AS}(K_{A,TGS}, K_{AS,TGS}(A, K_{A,TGS}))$
4
password?
5
PWD
6
$K_{AS,TGS}(A, K_{A,TGS}), B, K_{A,TGS}(t)$
7
$K_{A,TGS}(B, K_{A,B}), K_{B,TGS}(A, K_{A,B})$

- Authentication in Kerberos.

Example: Kerberos (2)



SESAME Components



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.

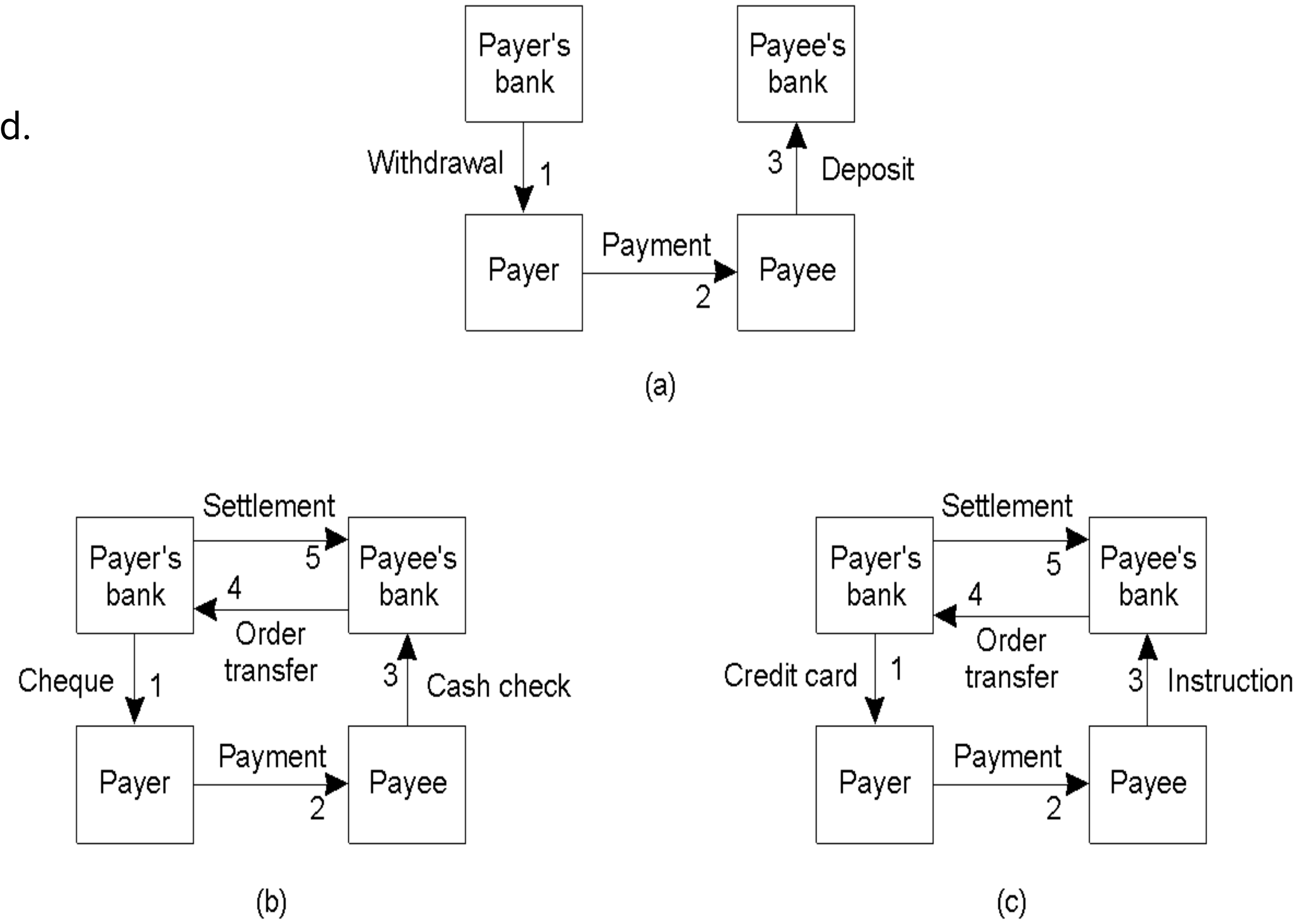
Electronic Payment Systems (1)

- Payment systems based on direct payment between customer and merchant.

a) Paying in cash.

b) Using a check.

c) Using a credit card.

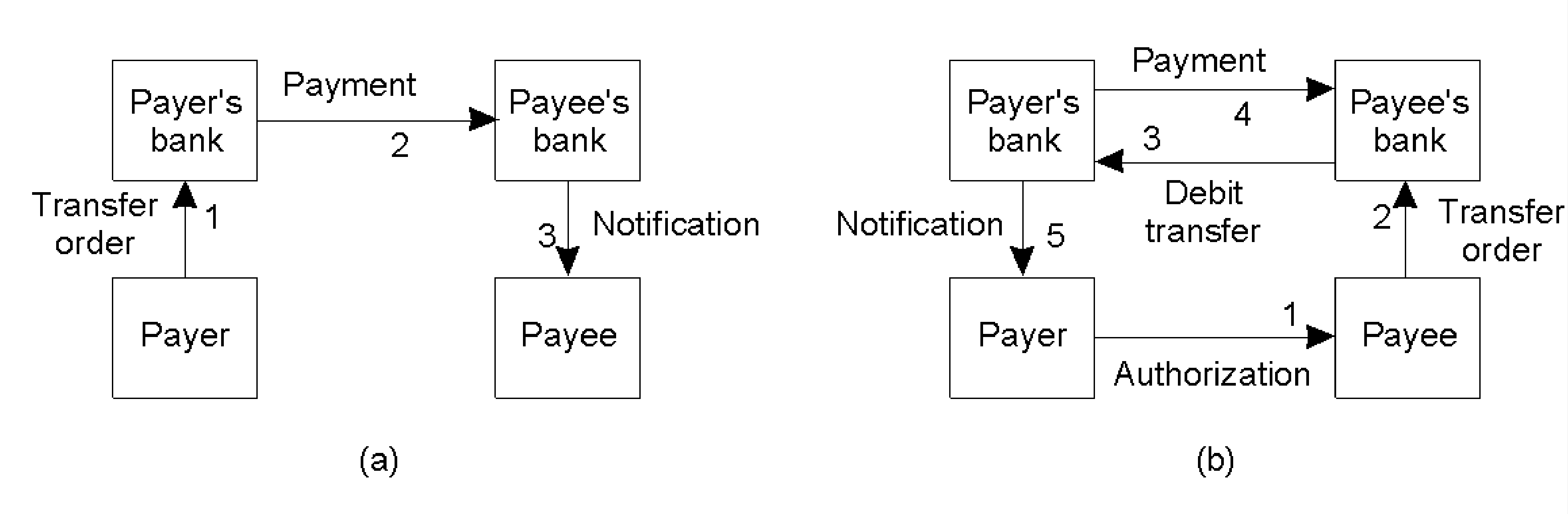


(a)

(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)

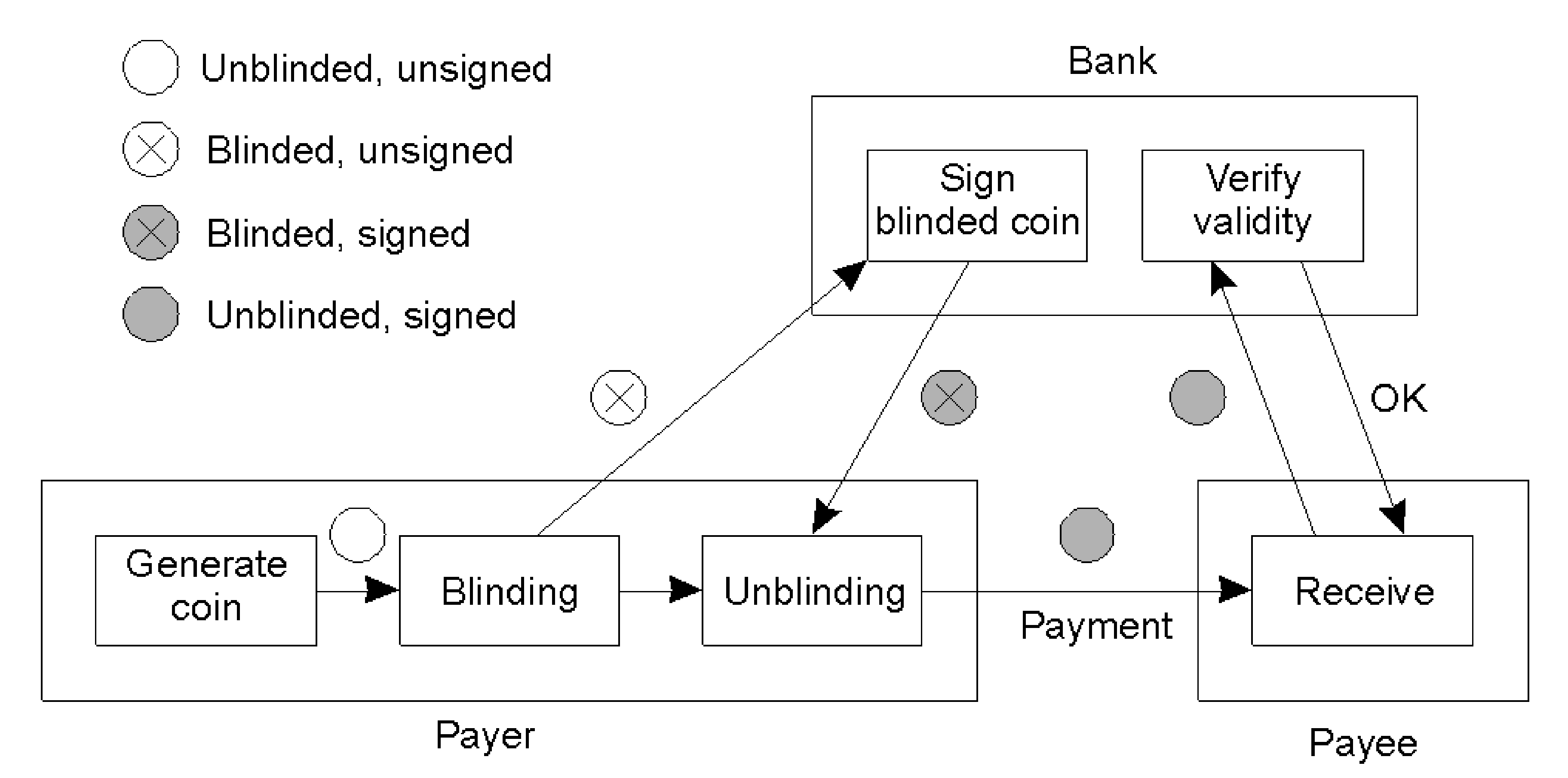
- Information hiding in a traditional credit-card system (see also [camp.lj96a])

Information

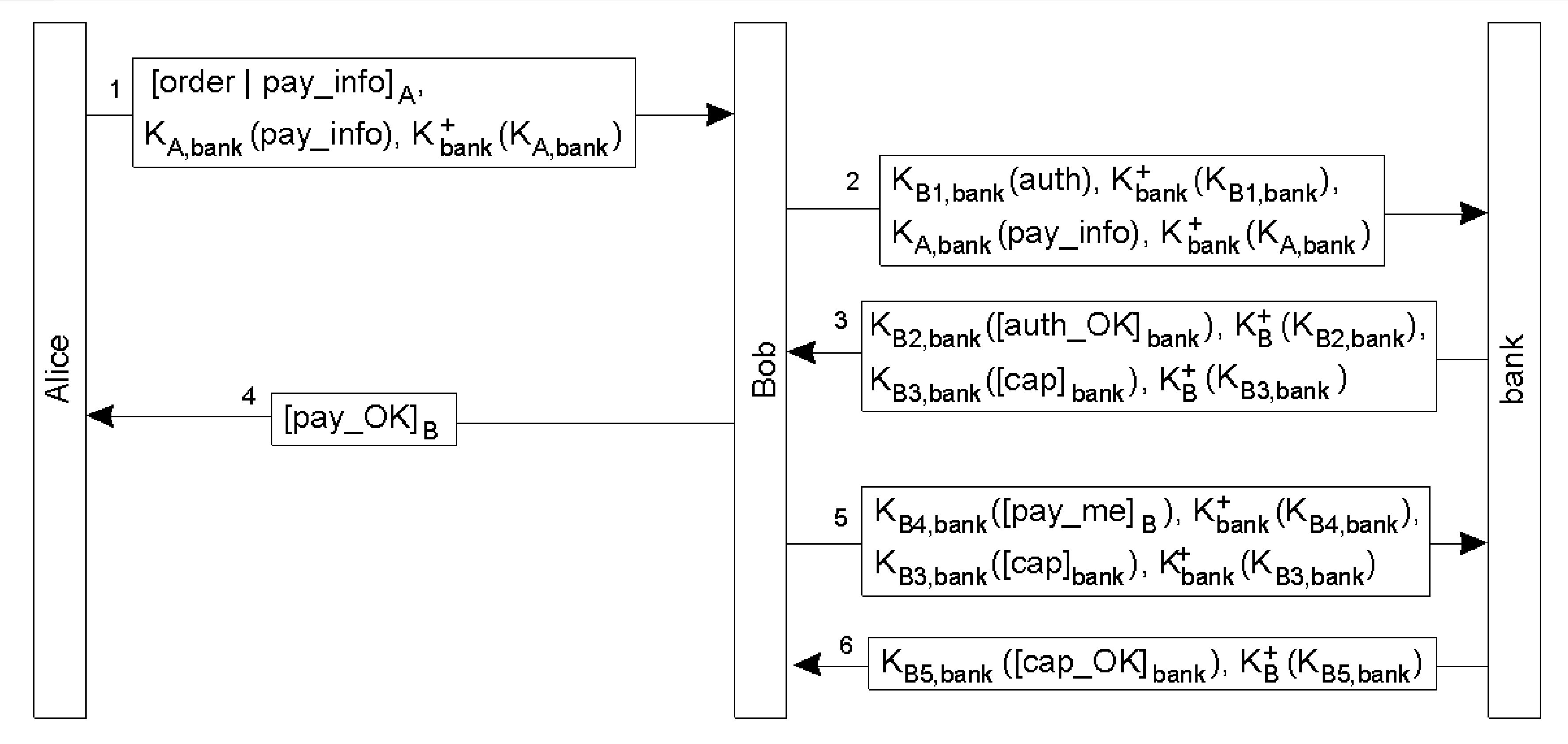
Party

	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

E-cash


Unblinded, unsigned
Blinded, unsigned
Blinded, signed
Unblinded, signed
Bank
Sign blinded coin
Verify validity
OK
Generate coin
Blinding
Unblinding
Payment
Receive
Payer
Payee

Secure Electronic Transactions (SET)



1 $[\text{order} \mid \text{pay\_info}]_A$, $K_{A,bank}(\text{pay\_info})$, $K^+_{bank}(K_{A,bank})$

2 $K_{B1,bank}(\text{auth})$, $K^+_{bank}(K_{B1,bank})$, $K_{A,bank}(\text{pay\_info})$, $K^+_{bank}(K_{A,bank})$

3 $K_{B2,bank}([\text{auth\_OK}]_{bank})$, $K^+_B(K_{B2,bank})$, $K_{B3,bank}([\text{cap}]_{bank})$, $K^+_B(K_{B3,bank})$

4 $[\text{pay\_OK}]_B$

5 $K_{B4,bank}([\text{pay\_me}]_B)$, $K^+_{bank}(K_{B4,bank})$, $K_{B3,bank}([\text{cap}]_{bank})$, $K^+_{bank}(K_{B3,bank})$

6 $K_{B5,bank}([\text{cap\_OK}]_{bank})$, $K^+_B(K_{B5,bank})$