

# Inventing the Future of Network Society by Information Security

The slide features several decorative circles. There are two solid light purple circles in the top row, one on the left and one on the right. Below them are two more solid light purple circles, also one on the left and one on the right. Additionally, there are two thin, light purple outlined circles: one in the top row on the right side, and one in the bottom row on the right side, partially overlapping the text.

Tatsuaki Okamoto  
(NTT)

The image features six light purple circles arranged in two rows. The top row contains three circles, and the bottom row contains three circles. The text 'Information Security' is centered horizontally between the two rows, overlapping the middle circles of both rows. The top-left circle is an outline, while the other five are solid.

# Information Security

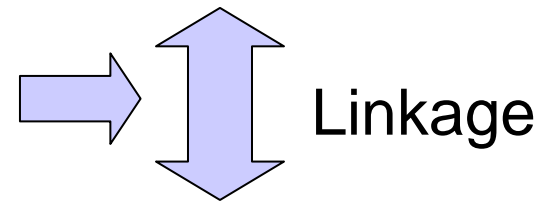
# The Role of Cryptography and Information Security

ICT systems . . .

(Every information is communicated and recorded by digital data)

Virtual World

Cryptography and Information Security



Real World  
(estate, property,  
bank account  
balance etc.)

# Cryptography and Information Security

- **Protecting Systems**

- Protect systems and databases from hackers to intrude and attack

- **Promoting Business over Networks**

- Payment via networks (**correctness**)
- Signing and contracting via networks

- **Promoting Social Activities over Networks**

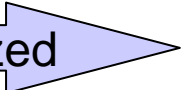
- Voting and auction via networks (**privacy**)

- **Promoting Entertainment over Networks**

- Coin flipping and lottery over networks (**fairness**)

# Cryptography: Key Technology in Information Security

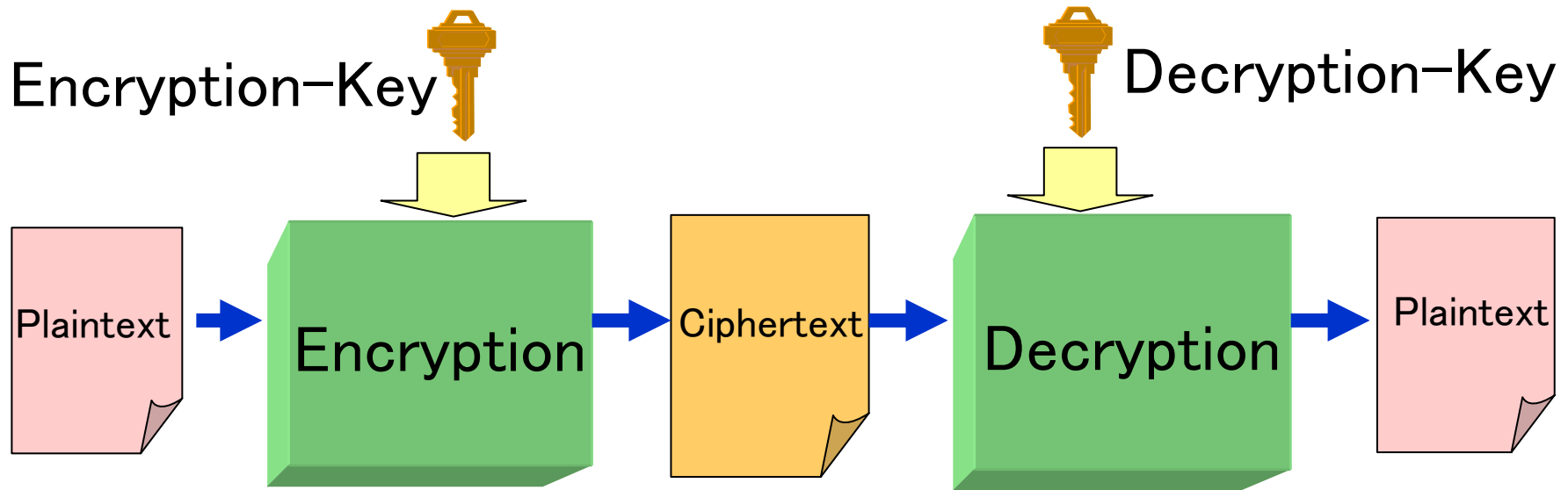
- Basic primitives
  - Confidentiality (Encryption, Key distribution)
  - Authentication (Signatures)
- Cryptographic Protocols
  - Privacy-enhanced basic-primitives
  - Electronic voting
  - Electronic payment/money
  - Electronic contracting
  - Electronic gaming

Theoretically generalized  Multi-party protocols



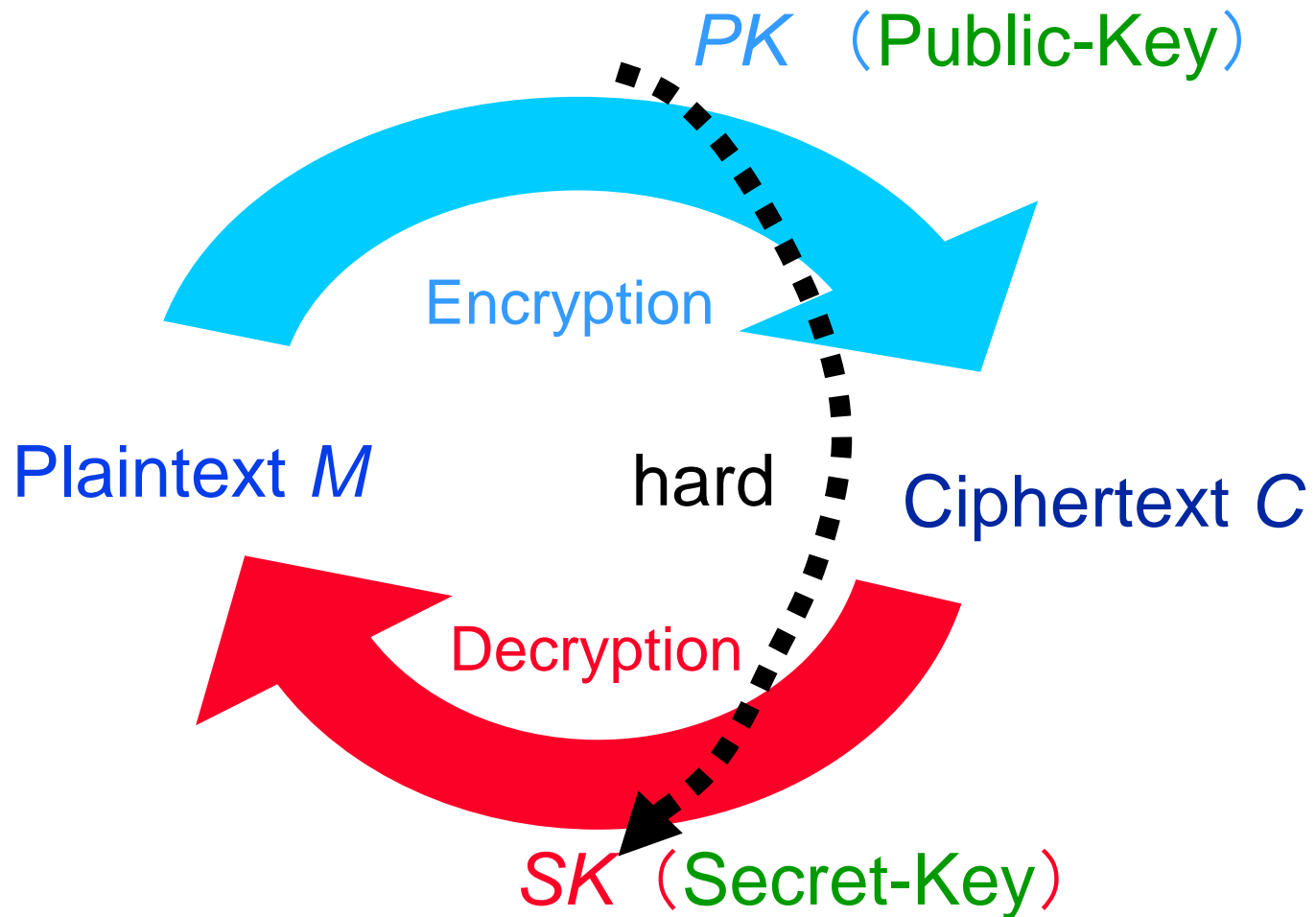
**Current Technology**

# Symmetric and Public-key Encryption



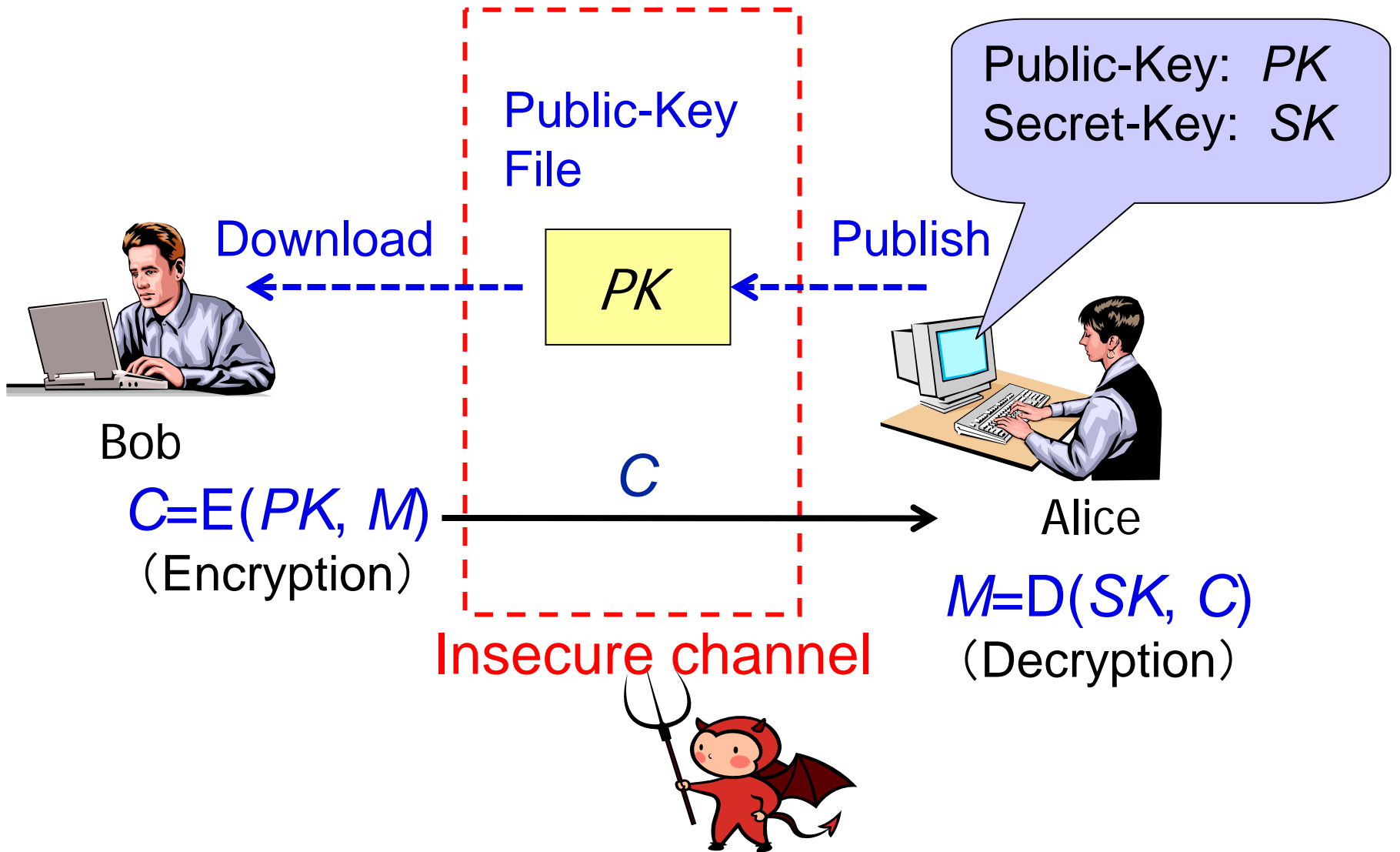
Symmetric Encryption	Encryption-Key = Decryption-Key
Public-key Encryption	Encryption-Key $\neq$ Decryption-Key

# Principle of Public-key Encryption

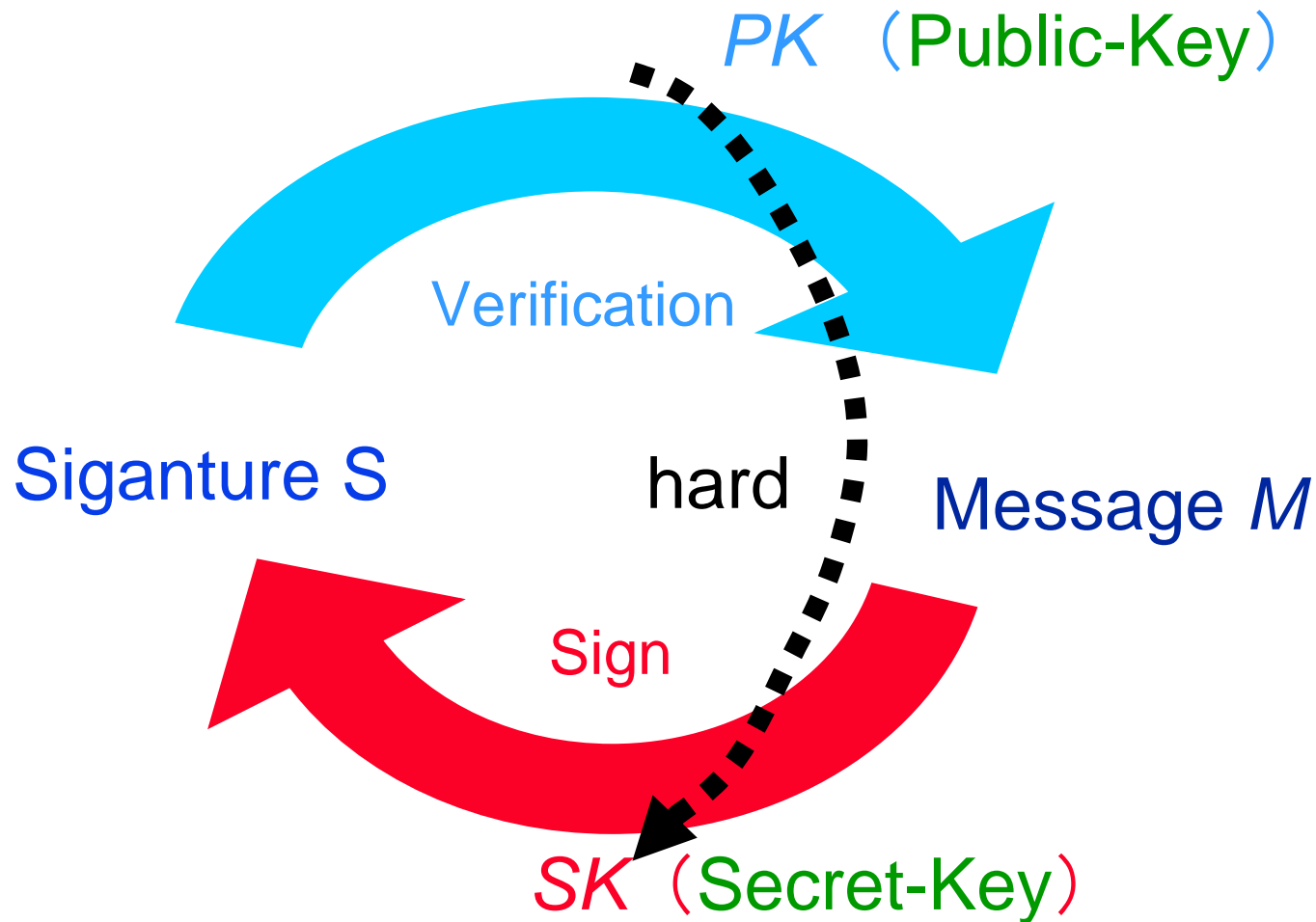




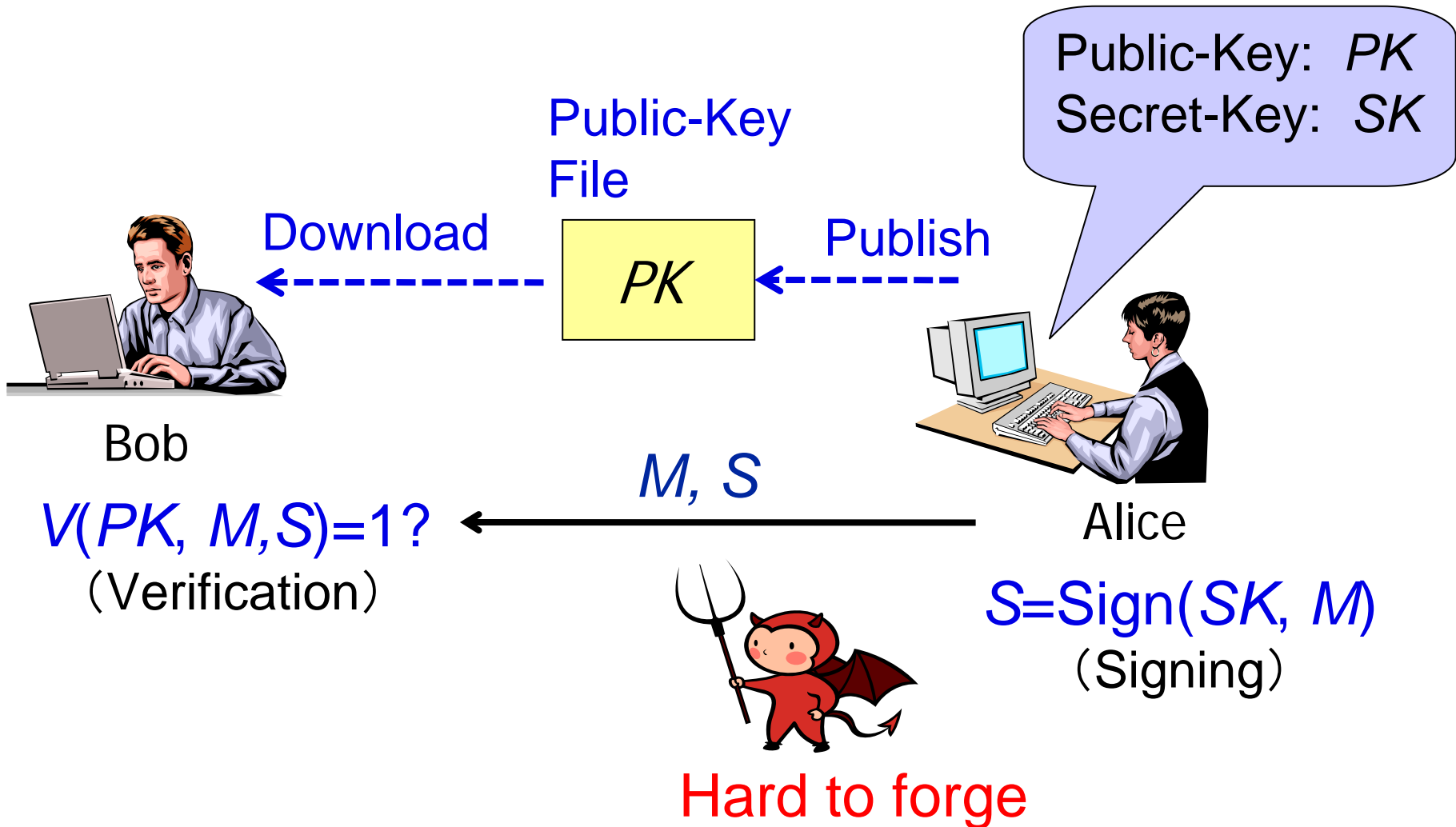
# Public-key Encryption



# Principle of Digital Signatures



# Digital Signatures



# Public-Key Infrastructures (PKI) Certification Authority (CA)

Organization to certify a public-key

Secret-Key Public-Key

SK



PK



Register Public-Key PK

Certification  
Authority (CA)



User A

Certifying PK  
with User A



CA's Sign



After confirming the  
identity of User A,  
issues the certification



**New Technology**

**(for New Network Services  
like Cloud Computing)**

# Virtual Private Network Service

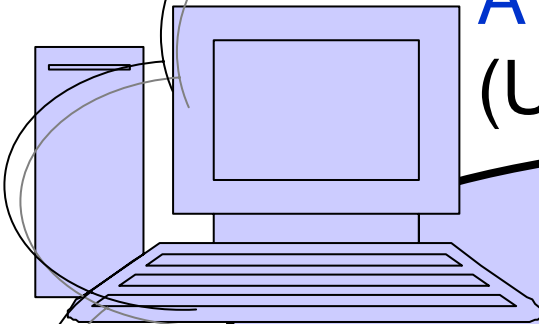
A Server Providing a Network Service  
(Using Secret Know-How to Operate)

Network Service  
on Accounting

Virtual Private Network Service

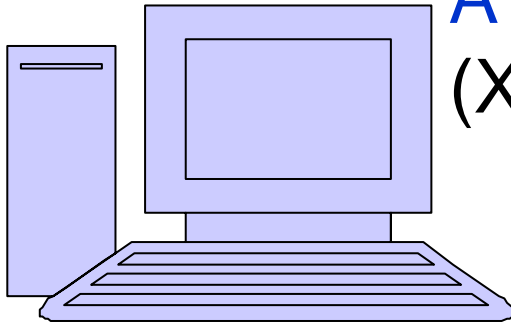
Private Data

User



# Virtual Private Network Service

A Server Providing a Network Service  
(X: Secret Know-How to Operate)



X

by Multi-Party Protocols

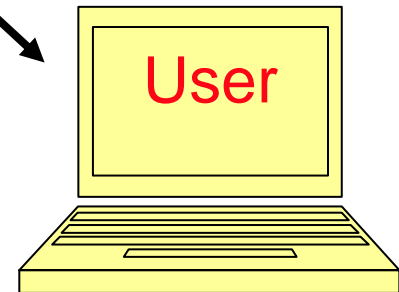
F: Computation of the Service

Y

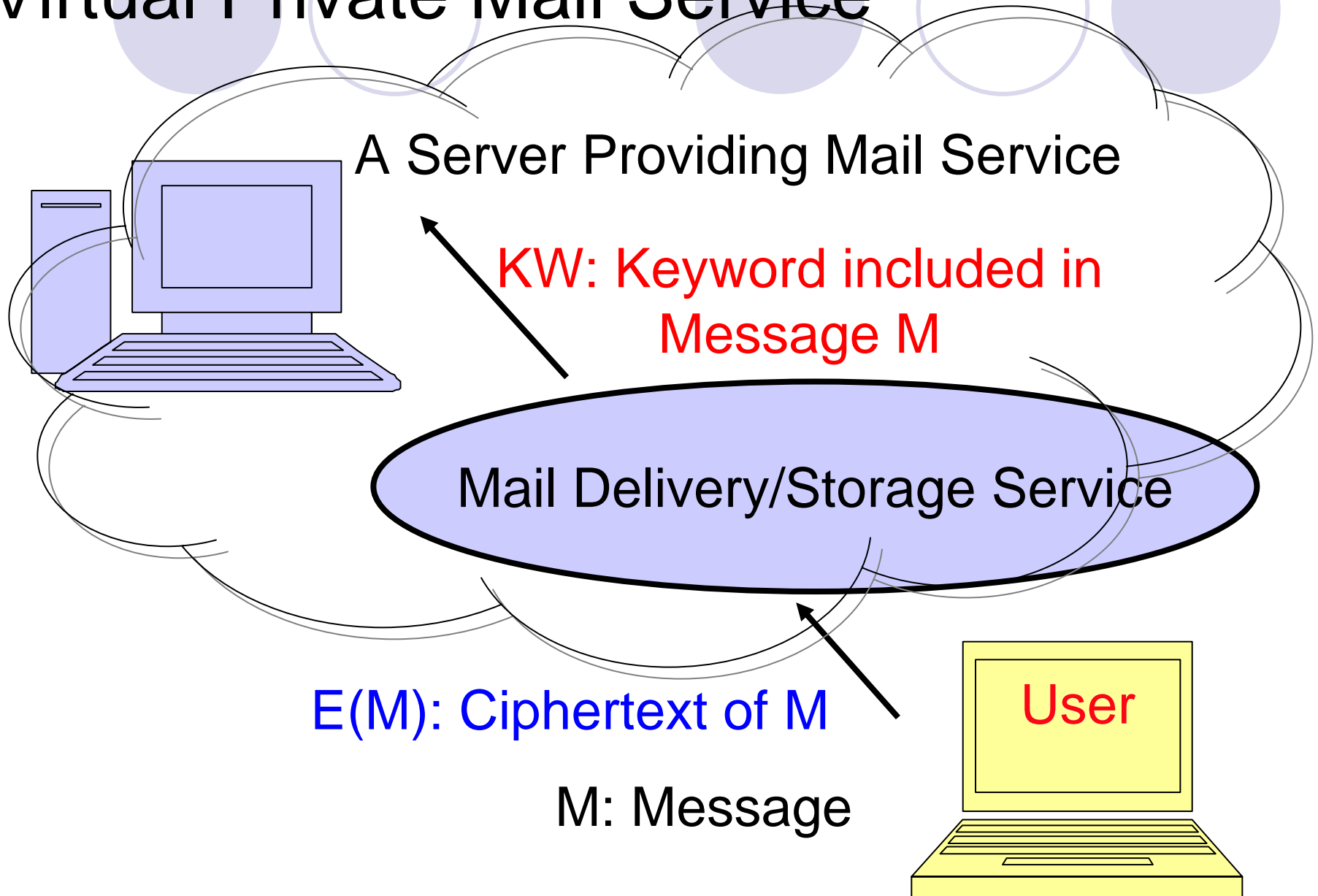
$F(X, Y)$

User

Y: Private Data

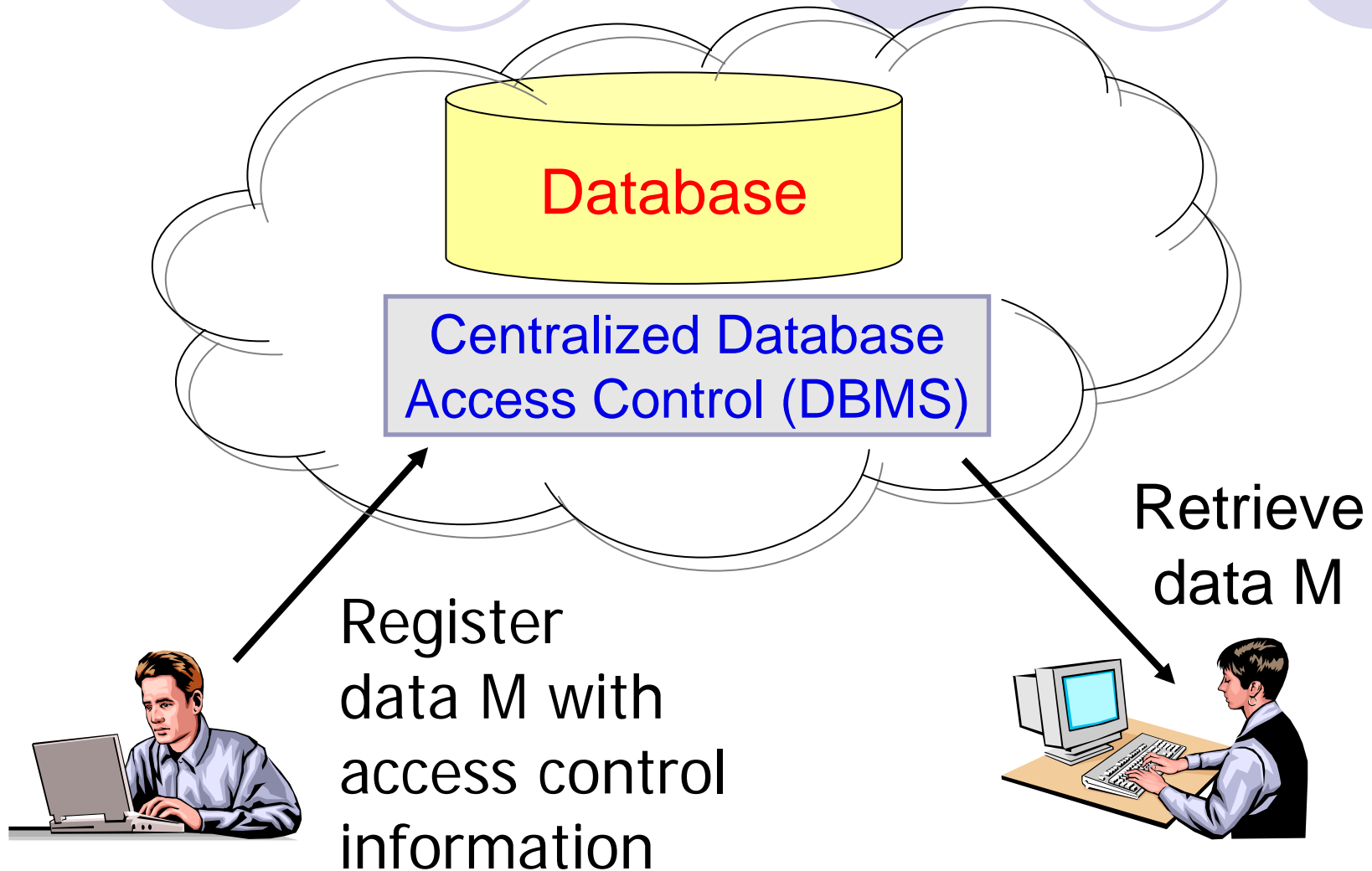


# Virtual Private Mail Service

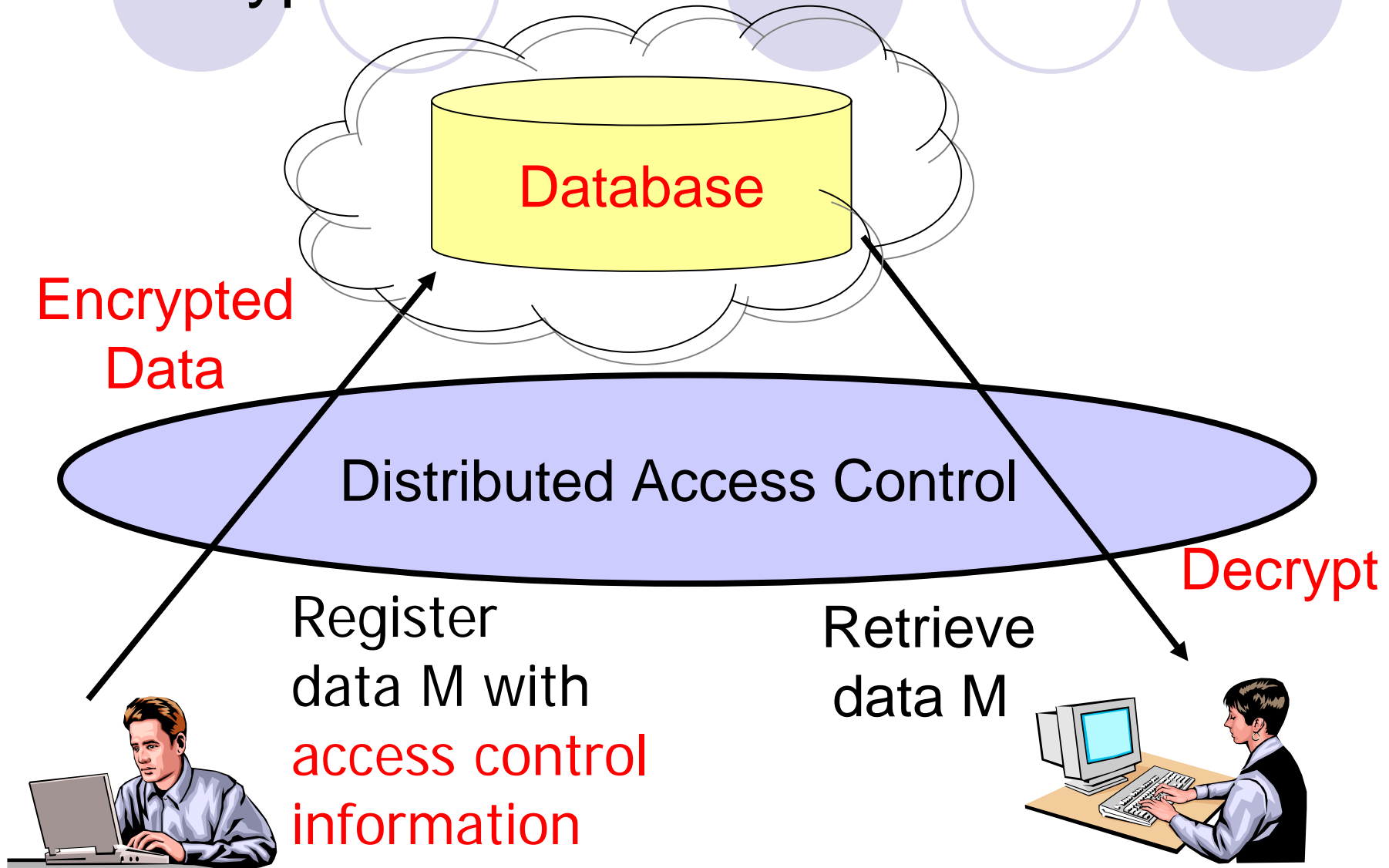




# Centralized Access Control of Database Services



# Distributed Access Control with Encryption for Database Services



# Advanced Encryption (Predicate Encryption)

Public-Key  
(system parameters)

$PK$

Publish

Public-Key:  $PK$   
Secret-Key:  $SK$   
(Master- $SK$ )



Authority

Download

Bob



Predicate  $f$

Secret-Key  
for  $f$   
( $SK_f$ )



Alice

$$C = E(x, PK, M)$$

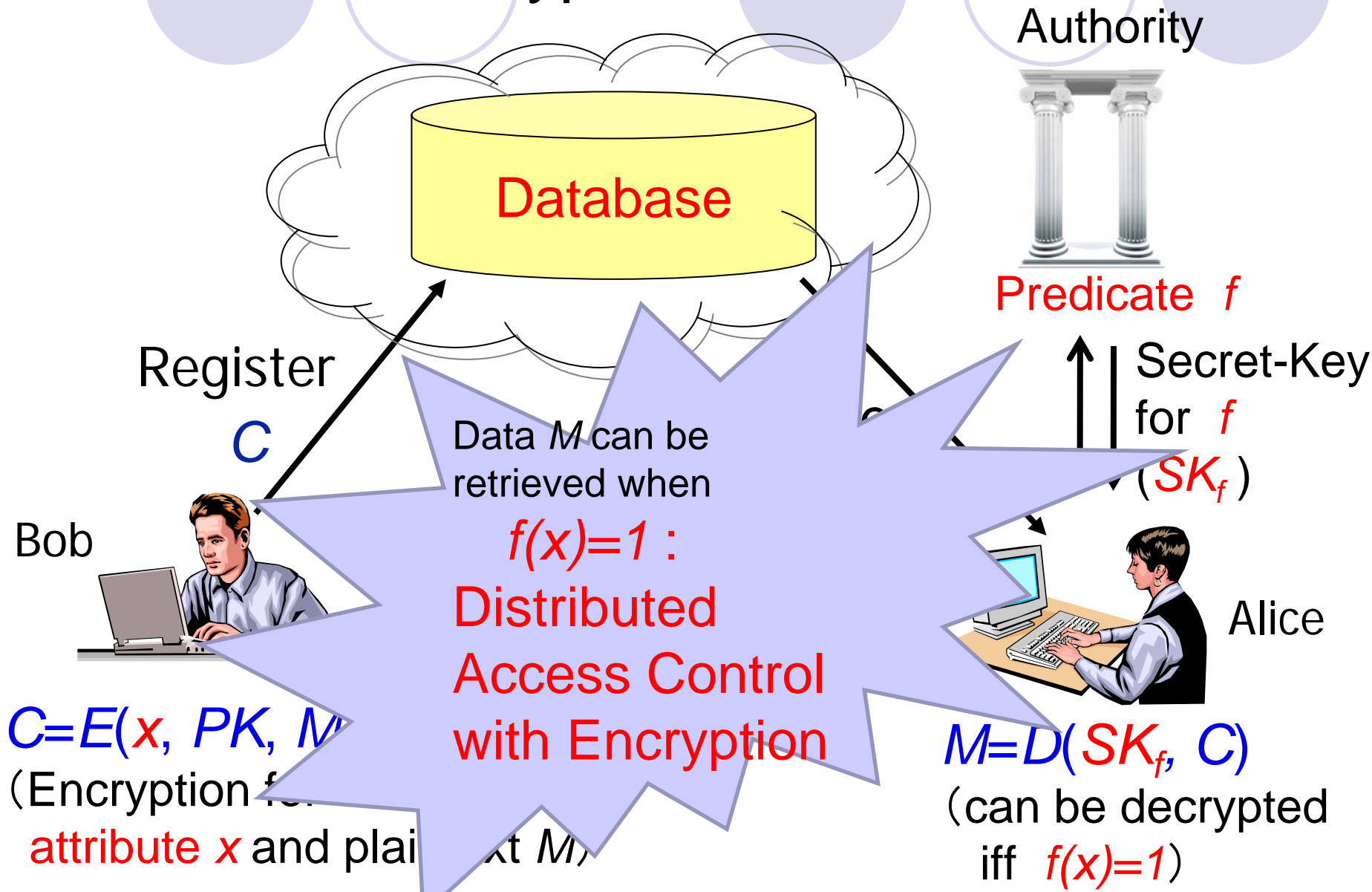
(Encryption for  
attribute  $x$  and plaintext  $M$ )

$C$

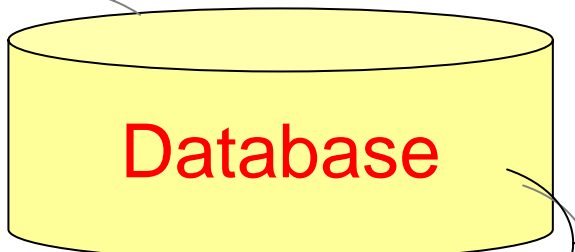
$$M = D(SK_f, C)$$

(can be decrypted  
iff  $f(x) = 1$ )

# Distributed Access Control by Advanced Encryption



Authority



Database

Register

C

Bob



Data  $M$  can be retrieved when

$$f(x)=1 :$$

Distributed Access Control with Encryption

Predicate  $f$

Secret-Key for  $f$

$(SK_f)$

Alice



$$C=E(x, PK, M)$$

(Encryption for attribute  $x$  and plaintext  $M$ )

$$M=D(SK_f, C)$$

(can be decrypted iff  $f(x)=1$ )

# Advanced Encryption 1 (Predicate Encryption)

Public-Key  
(system parameters)

$PK$

Publish



Public-Key:  $PK$   
Secret-Key:  $SK$   
(Master- $SK$ )



Authority

Download

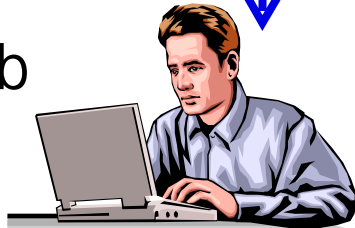


Predicate  $f =$   
 $(X=Animation) \wedge$   
 $(Y=Price\ Zone\ 2 \vee Z=Class\ 1)$



Secret-Key  
for  $f$   
 $(SK_f)$

Bob



Alice

$$C = E(x, PK, M)$$

(Encryption for

attribute  $x = (X, Y, Z) =$

(Animation, Price Zone 2, Class 2))

$C$



$$M = D(SK_f, C)$$

(can be decrypted

iff  $f(x)=1$ )

# Advanced Encryption 2 (Predicate Encryption)

Public-Key  
(system parameters)

$PK$

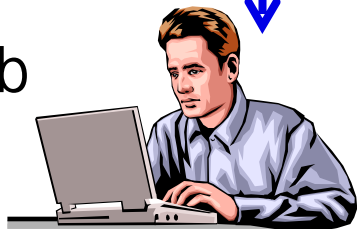
Publish



Download



Bob



$$C = E(f, PK, M)$$

(Encryption for

predicate  $f =$

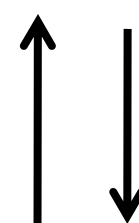
$X = \text{NTT} \wedge (Y < 35 \vee Z = \text{Male})$ )

Attribute  $x = (X, Y, Z) =$   
(NTT, Age:30, Female)

Public-Key:  $PK$   
Secret-Key:  $SK$   
(Master- $SK$ )



Authority



Secret-Key  
for  $x$   
( $SK_x$ )



Alice

$$M = D(SK_x, C)$$

(can be decrypted  
iff  $f(x) = 1$ )



$C$



# Summary

- How to guarantee the **security** in **new network services like cloud computing** is a key issue in promoting the services.
- **New cryptographic (information security) technology** guarantees and promotes **secure** networks services.
  - Multiparty protocols
  - Advanced encryption