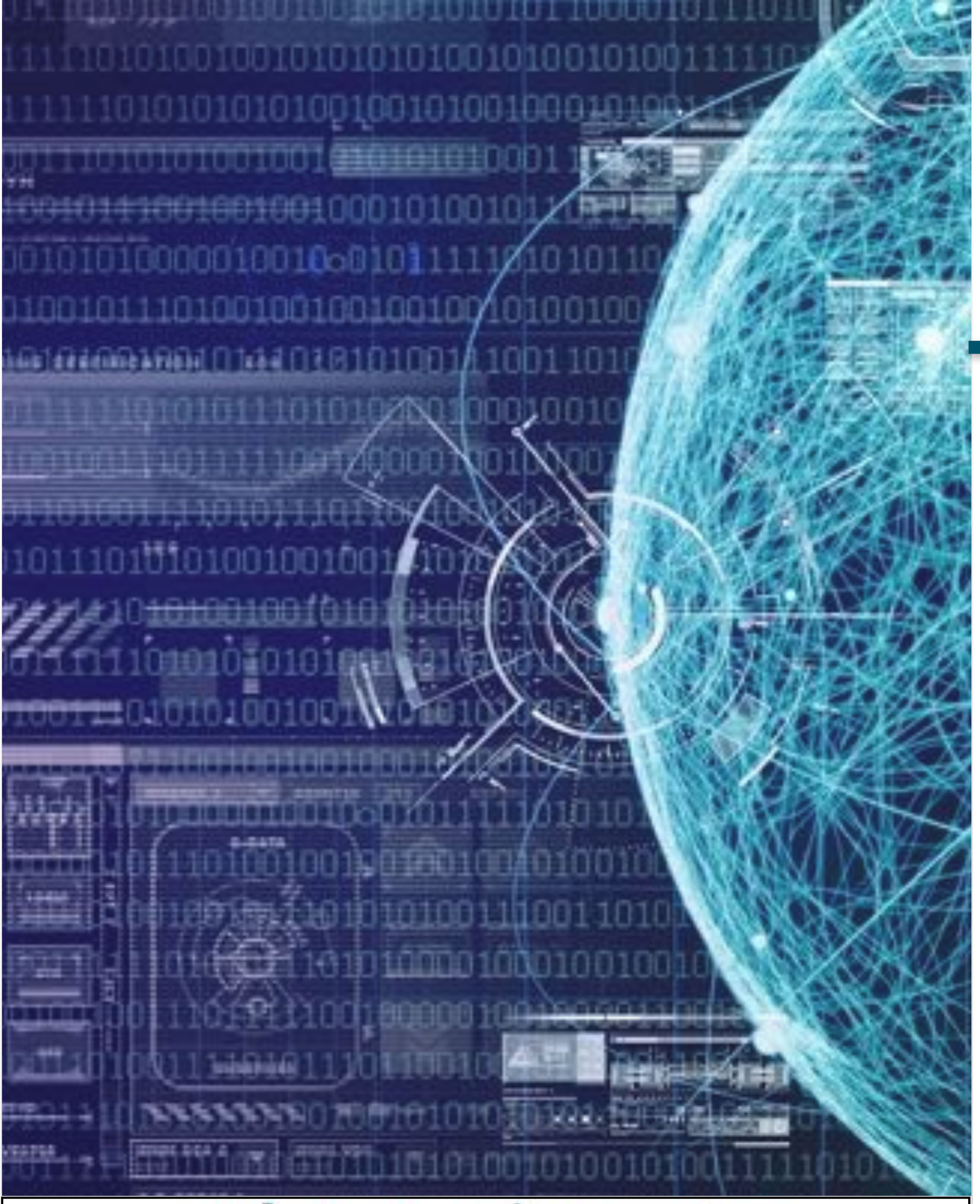


COMP6224(16)
week 2: introduction to crypto primitives and protocols

Vladimiro Sassone
Cyber Security Centre
University of Southampton

CyberSecuritySoton.org [w]

@CybSecSoton [fb & tw]

Topics in lecture

Primary network security issues

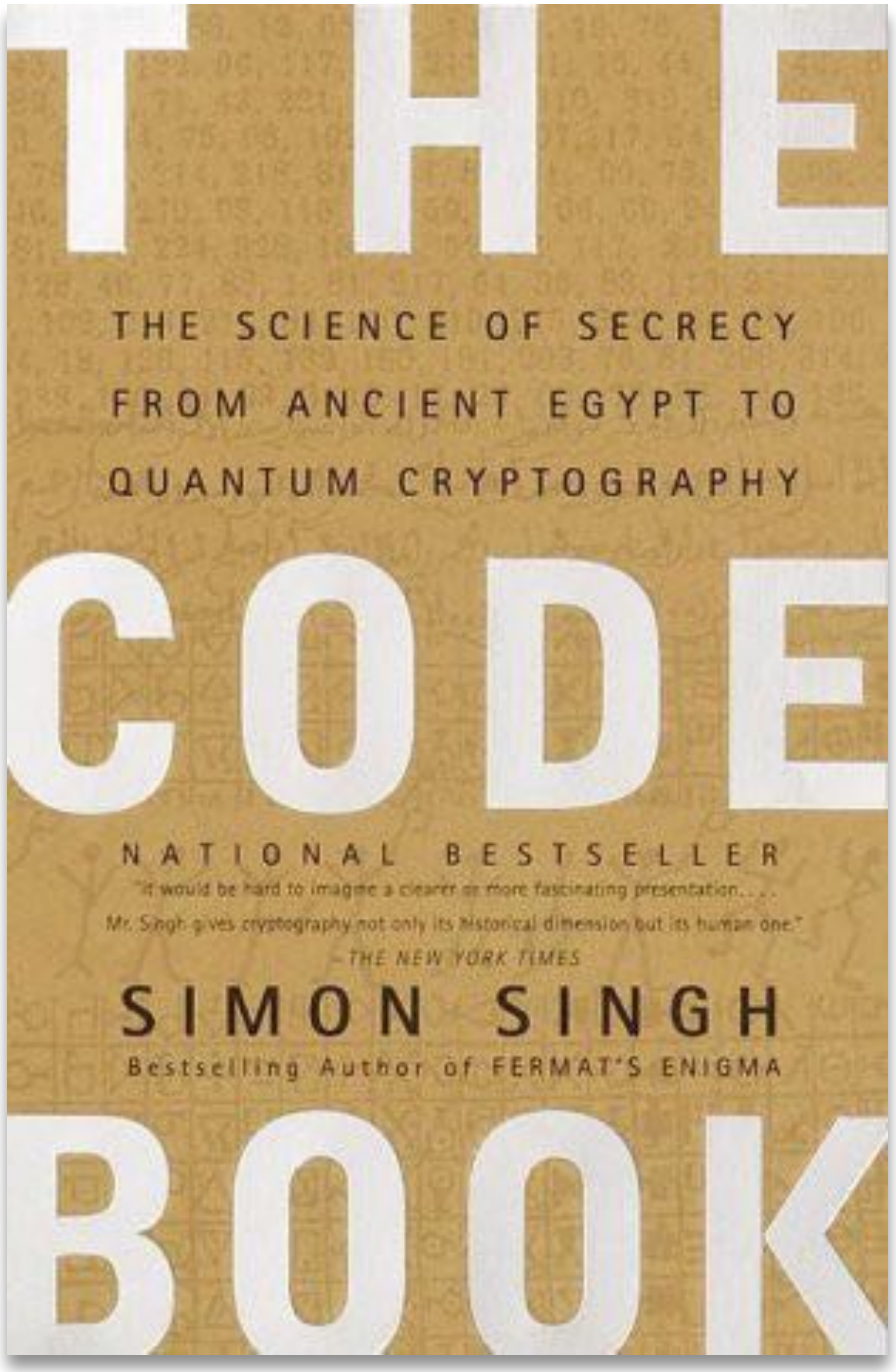
Cryptographic fundamentals

Two well known security protocols

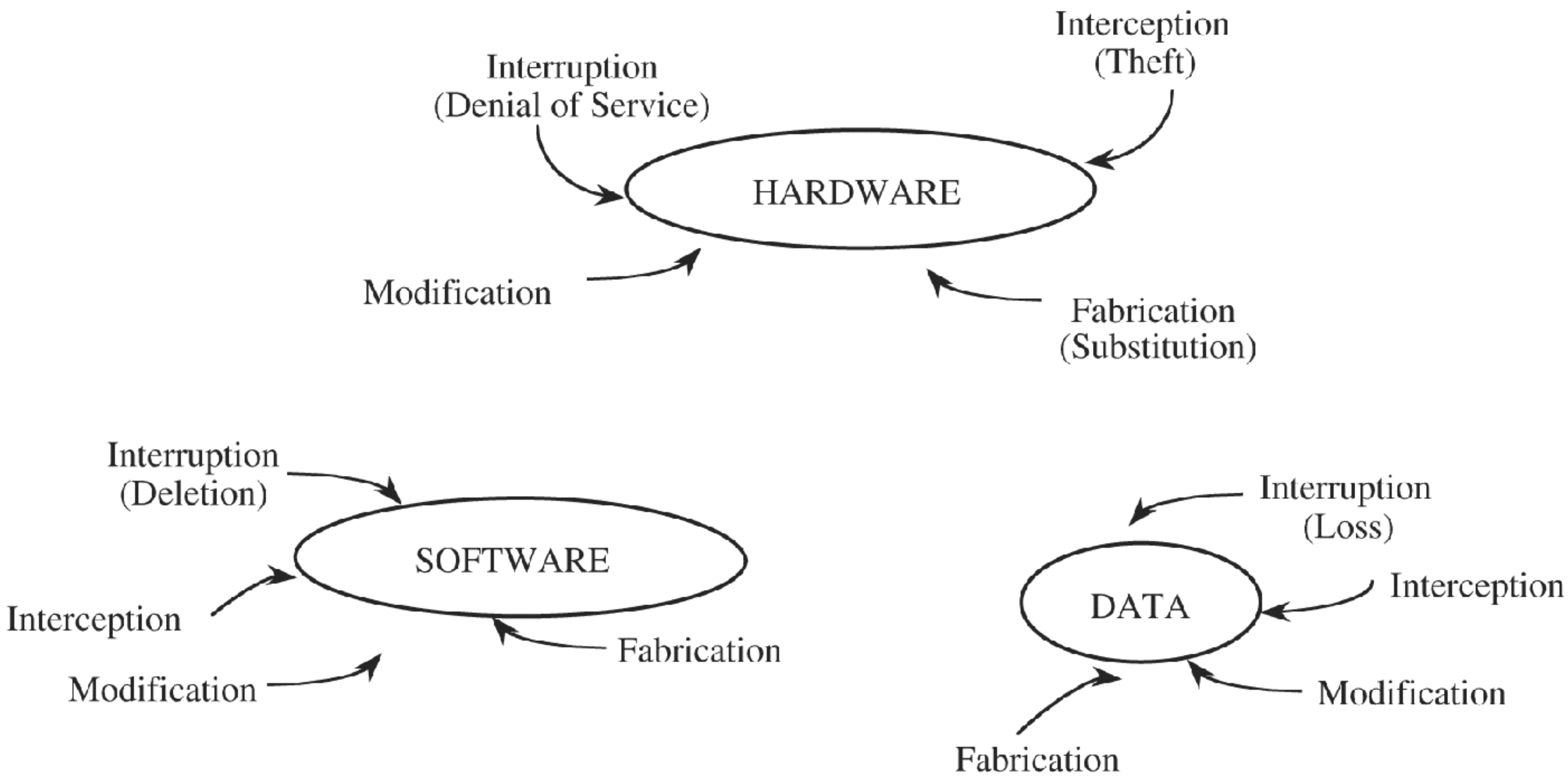
Primary network security issues

Cryptographic fundamentals

Two well known security protocols



Vulnerabilities of Computing Systems



Primary network security issues

Confidentiality – messages exchanged across network remains private

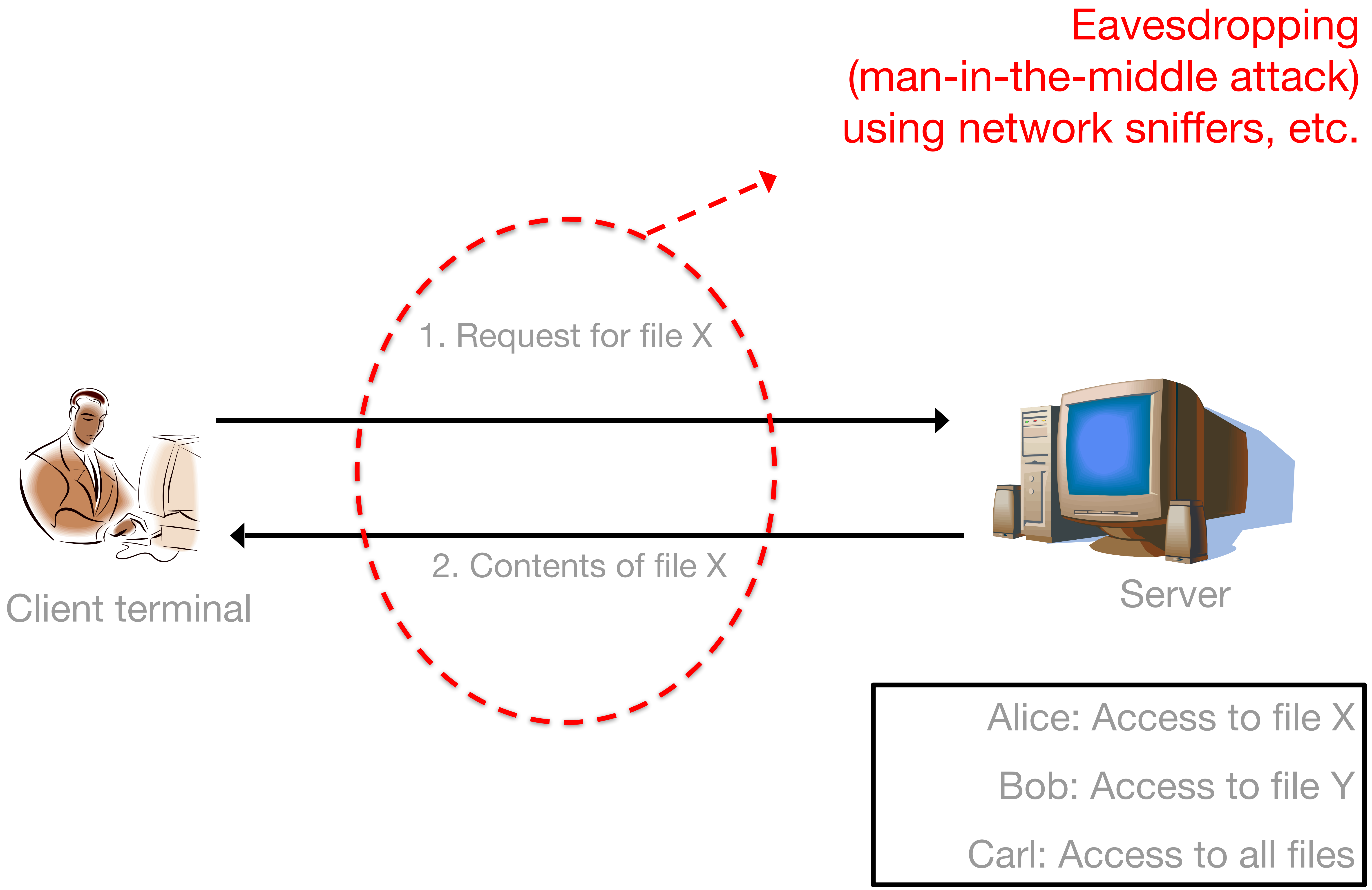
Integrity – contents of messages are not modified while in transit

Authentication – determining the identity of entities involved in message exchanges

Authorisation / Access control – determining the resources that an entities are allowed to access and in what manner

Non-repudiation – ensures that parties cannot deny having sent messages.

Primary network security issues



Topics in lecture

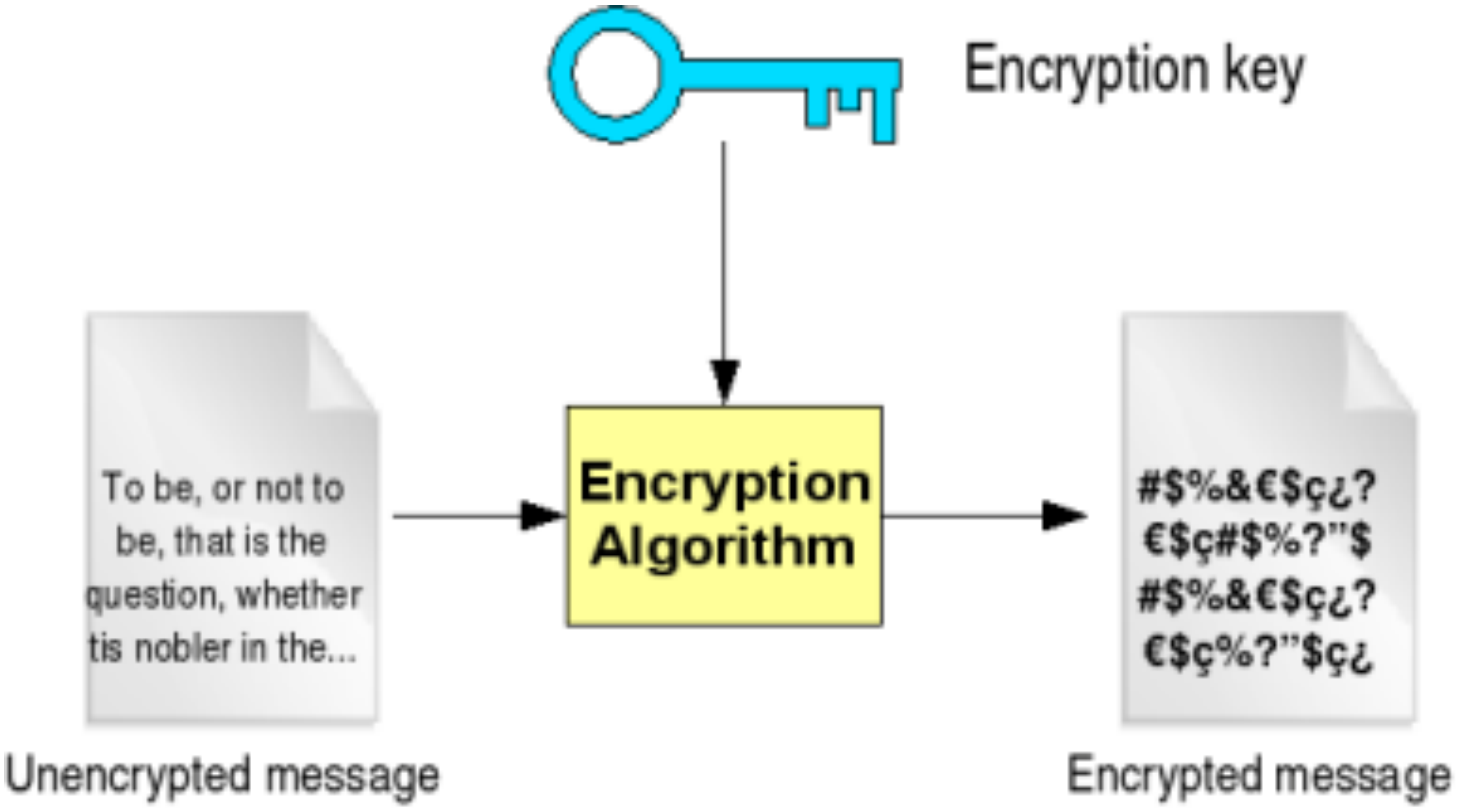
Primary network security issues

Cryptographic fundamentals

- **Symmetric/asymmetric encryption**
- Digital Signatures, Certificates and PKI

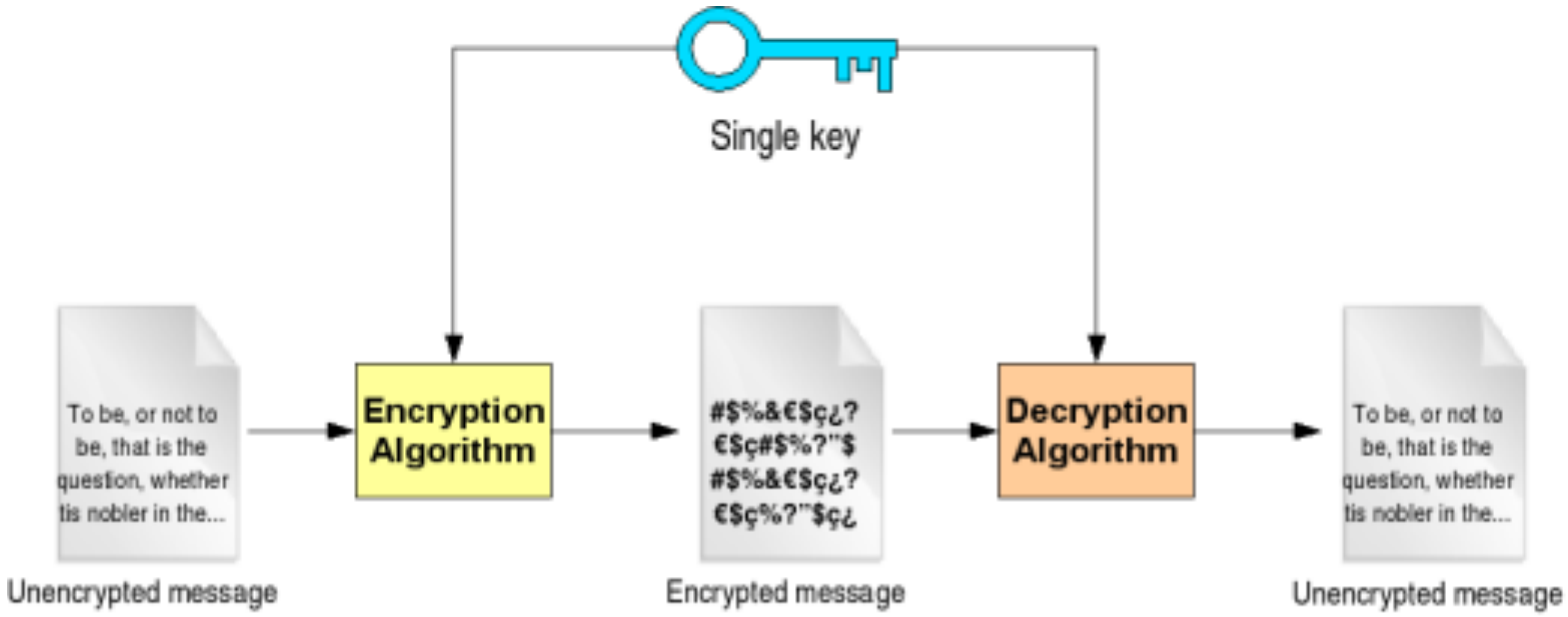
Two well known security protocols

- Addresses confidentiality
- Uses an encryption algorithm and an encryption key
- For a given plain text message, encrypted version will differ for different key sequences



Symmetric encryption

- "Same" key used for encrypting and decrypting
- Fast and simple to implement; stream/block ciphers
- Drawbacks: sender and receiver must agree on same key: the shared secret; quality of key generation
- Subject to attacks: known and chosen plaintext, differential and linear cryptanalysis
- Examples: 3DES, AES, RC4 (used in SSL and WEP)



Asymmetric encryption

Two types of keys: ***public*** and ***private***

Private key only known to entity, public key distributed openly

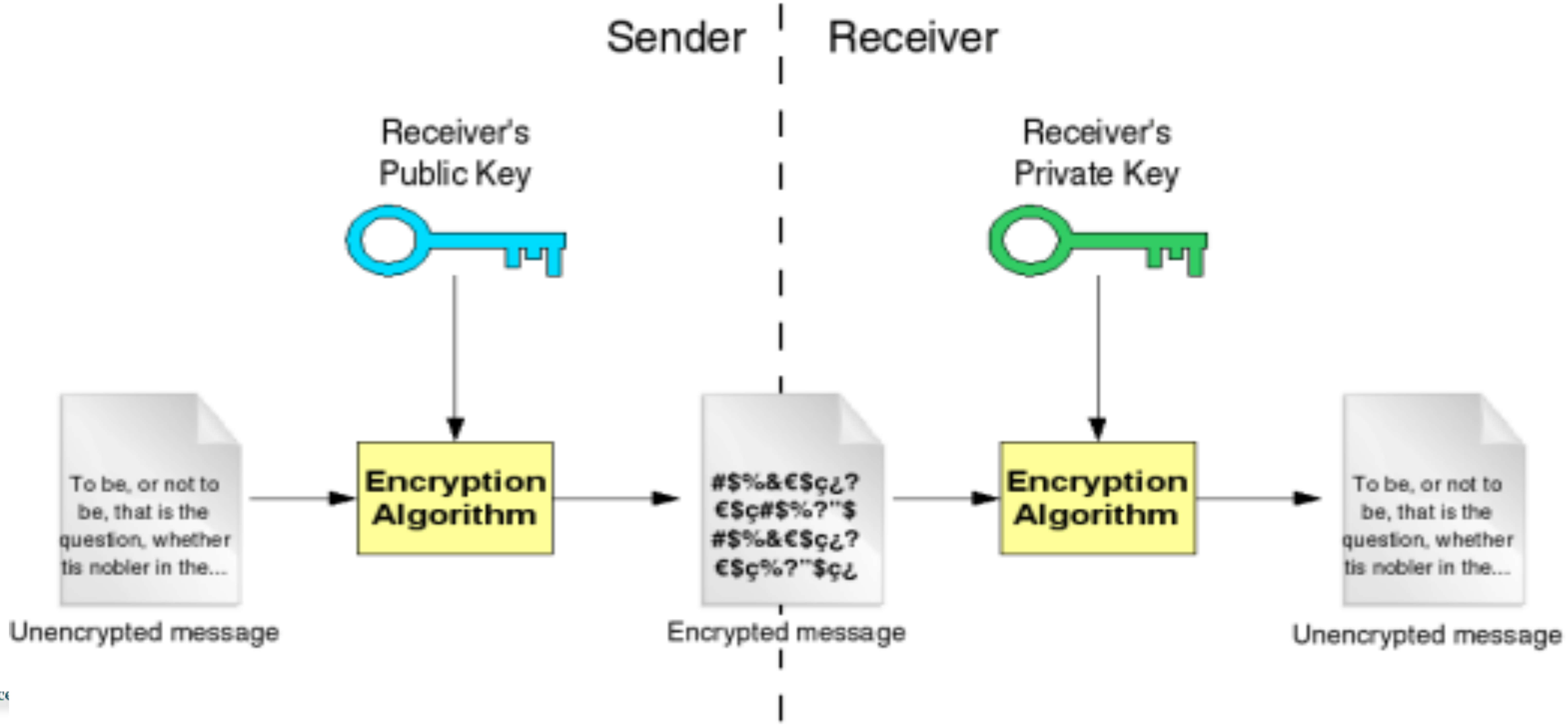
Encrypt by public key, decrypt by private key or vice versa easy

Generate public from private key easy, but not vice versa

Requires no shared secret; allows for *auth* & *non-rep & integrity*

Brute-force attacks; man-in-the-middle. *key distribution crucial*

Computationally harder than symmetric crypto; session keys



Substitution schemes: Caesar, …, Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Substitution schemes: Caesar, …, Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

ATTACKATDAWN

Substitution schemes: Caesar, …, Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

ATTACKATDAWN

\+

LEMON

Substitution schemes: Caesar, …, Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

ATTACKATDAWN

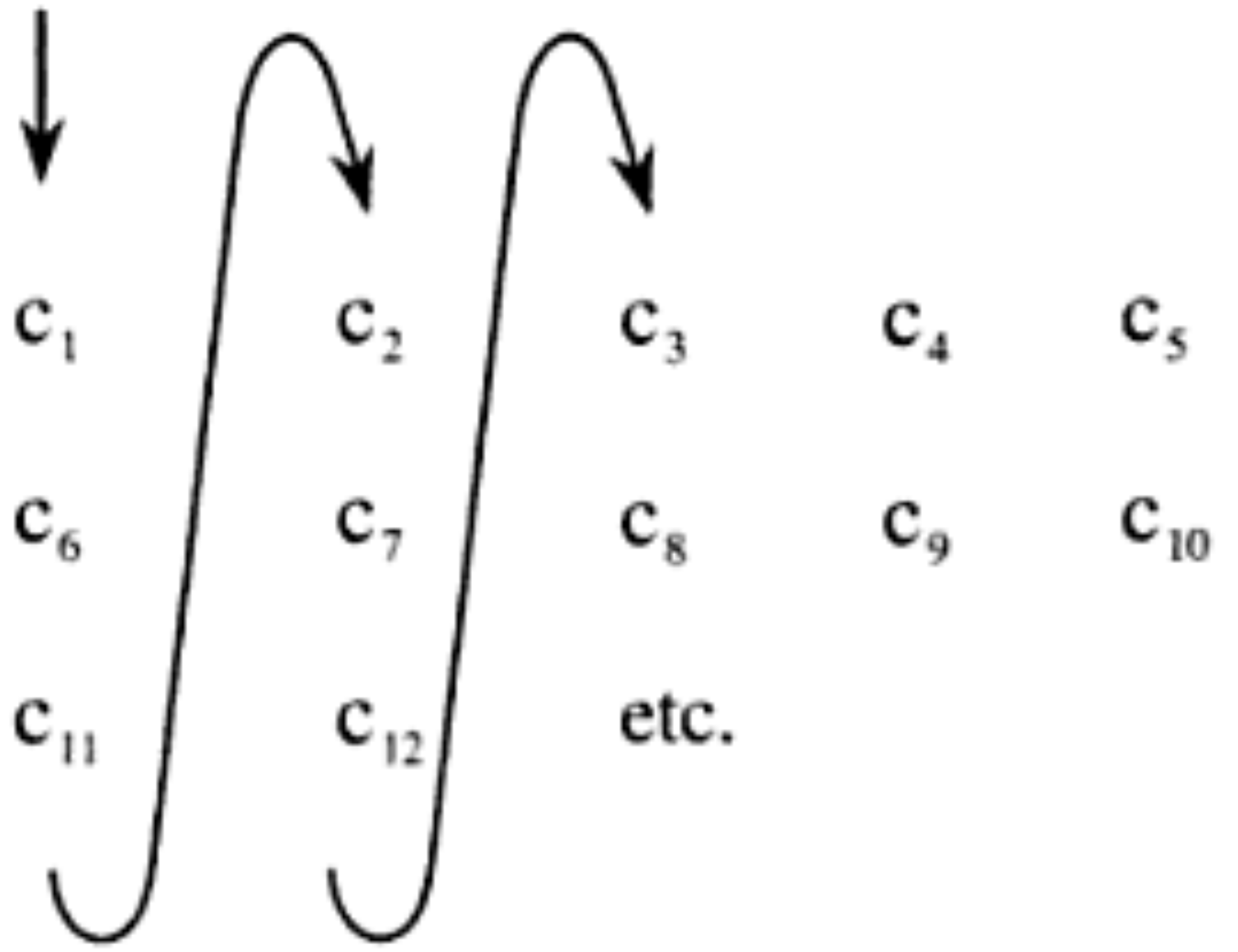
+

LEMON

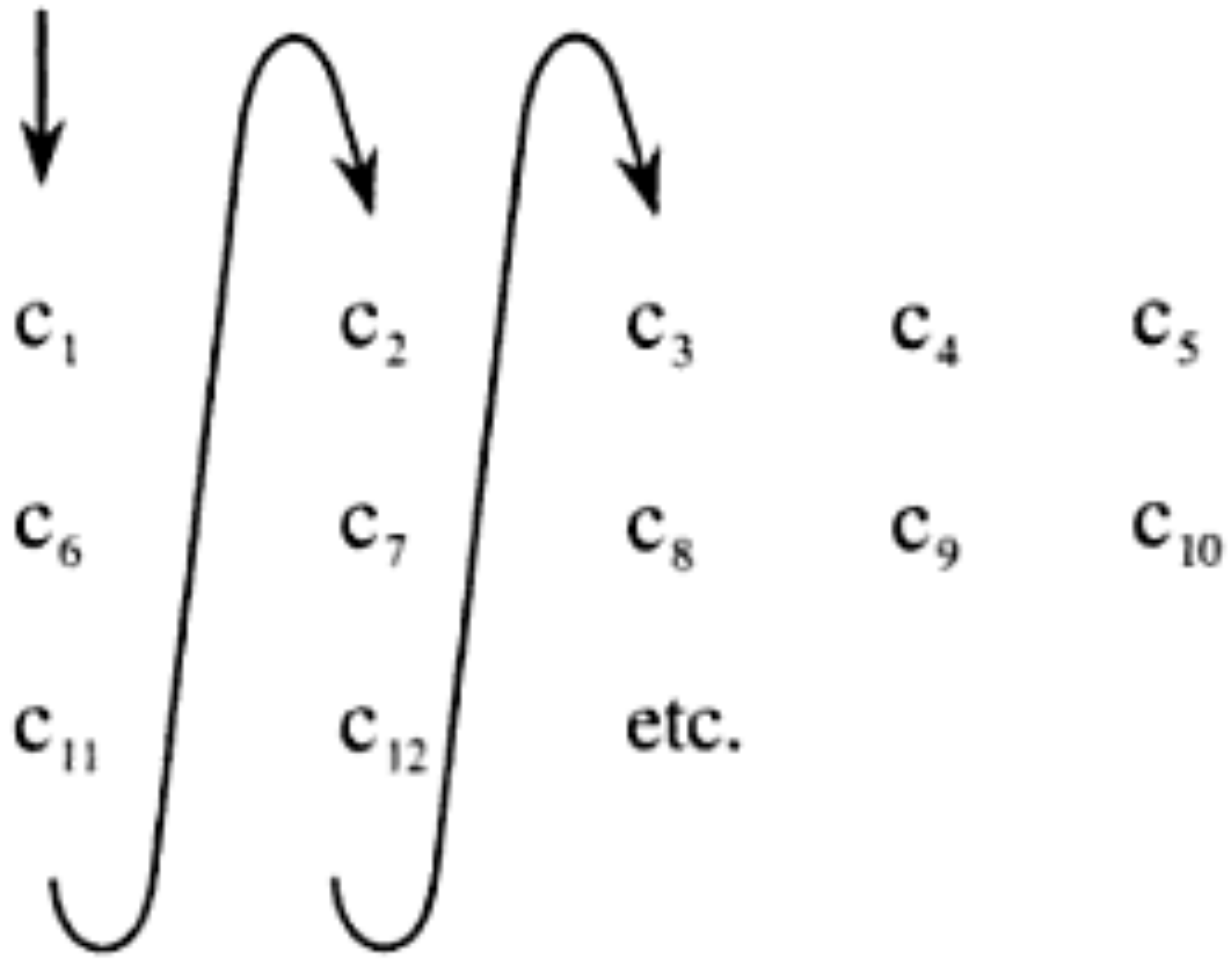
=

LXFOPVEFRNHR

Transposition schemes



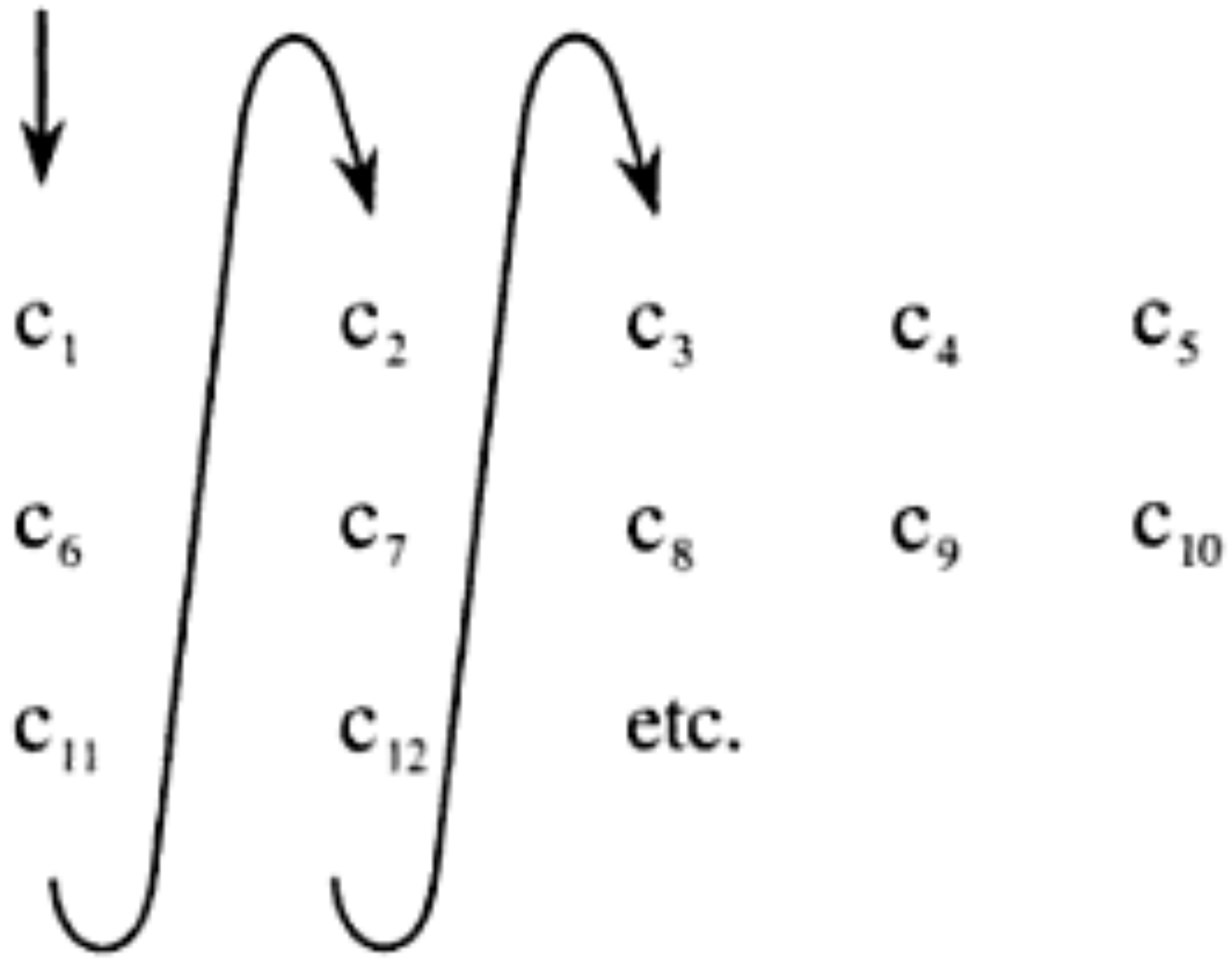
Transposition schemes



T	H	I	S	I
S	A	M	E	S
S	A	G	E	T
O	S	H	O	W
H	O	W	A	C
O	L	U	M	N
A	R	T	R	A
N	S	P	O	S
I	T	I	O	N
W	O	R	K	S

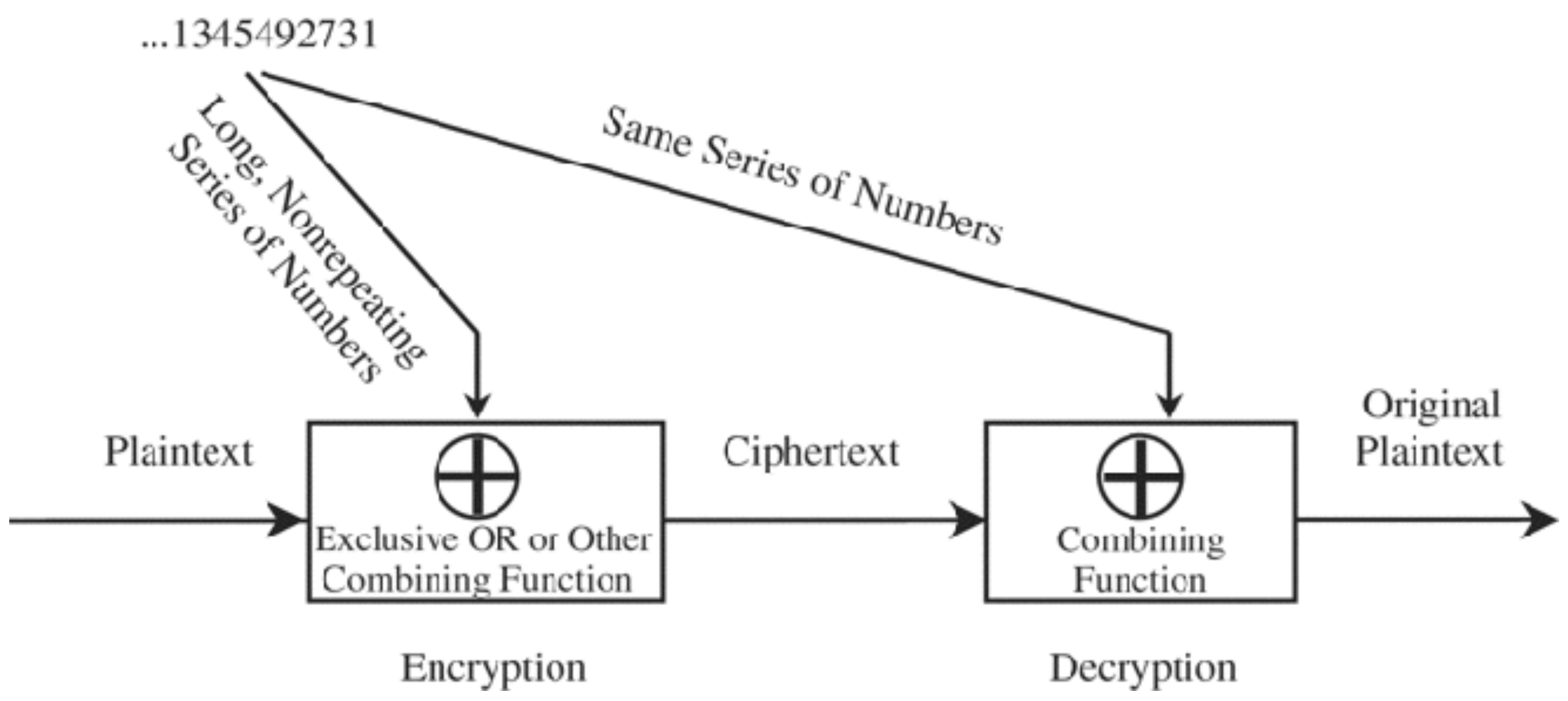
UNIVERSITY OF Southampton

Transposition schemes



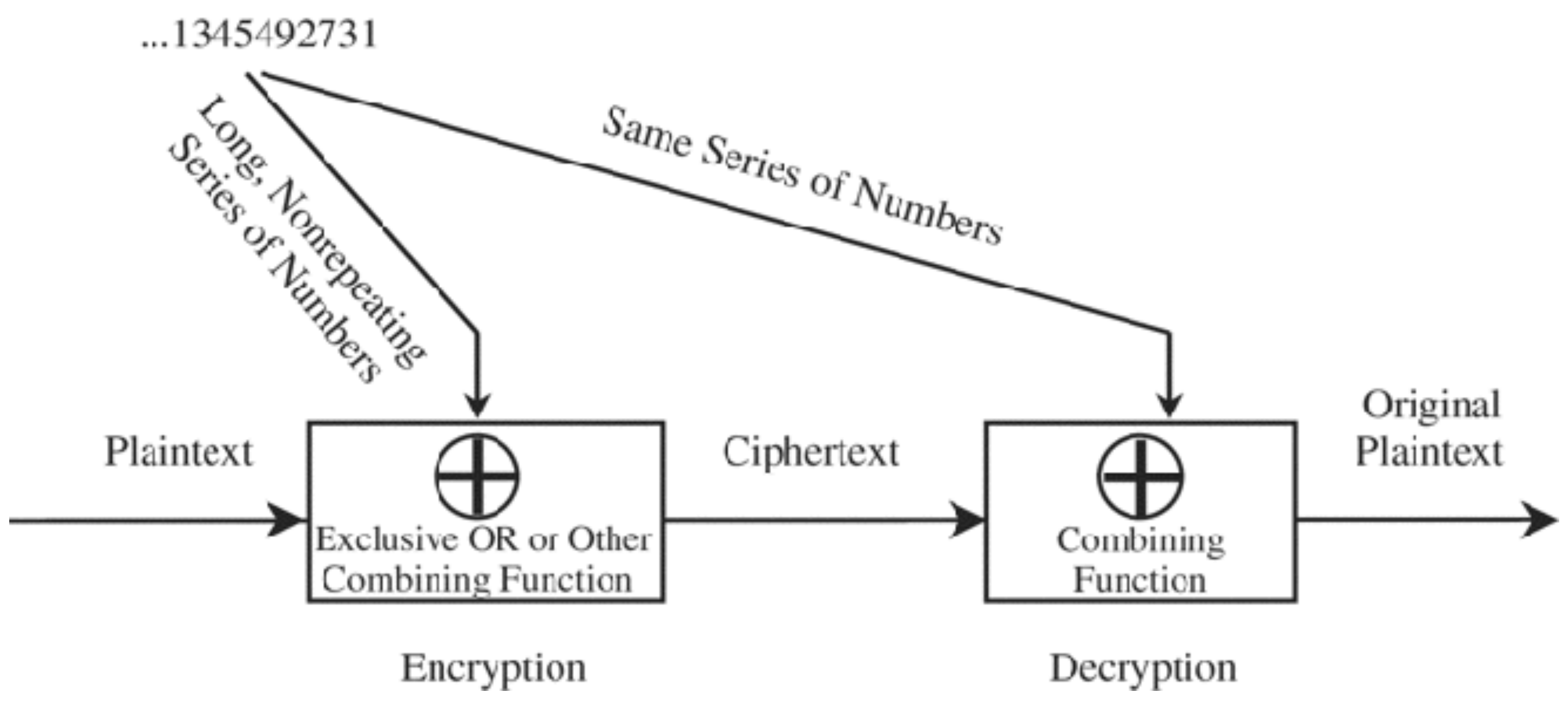
T	H	I	S	I
S	A	M	E	S
S	A	G	E	T
O	S	H	O	W
H	O	W	A	C
O	L	U	M	N
A	R	T	R	A
N	S	P	O	S
I	T	I	O	N
W	O	R	K	S

tssoh oaniw haaso lrsto imghw
utpir seeoa mrook istwc nasns



Vernam Cipher

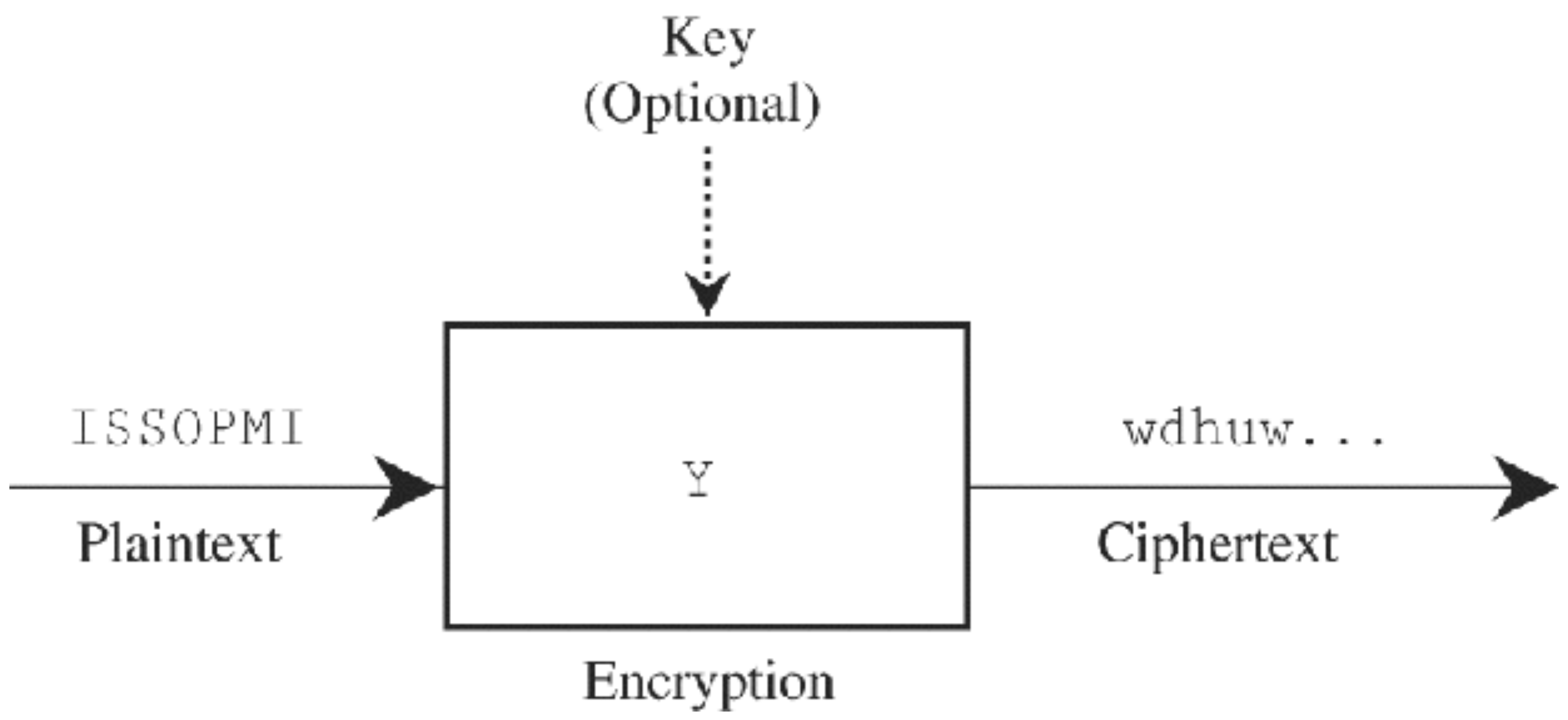
going digital: basic (over)simplified idea

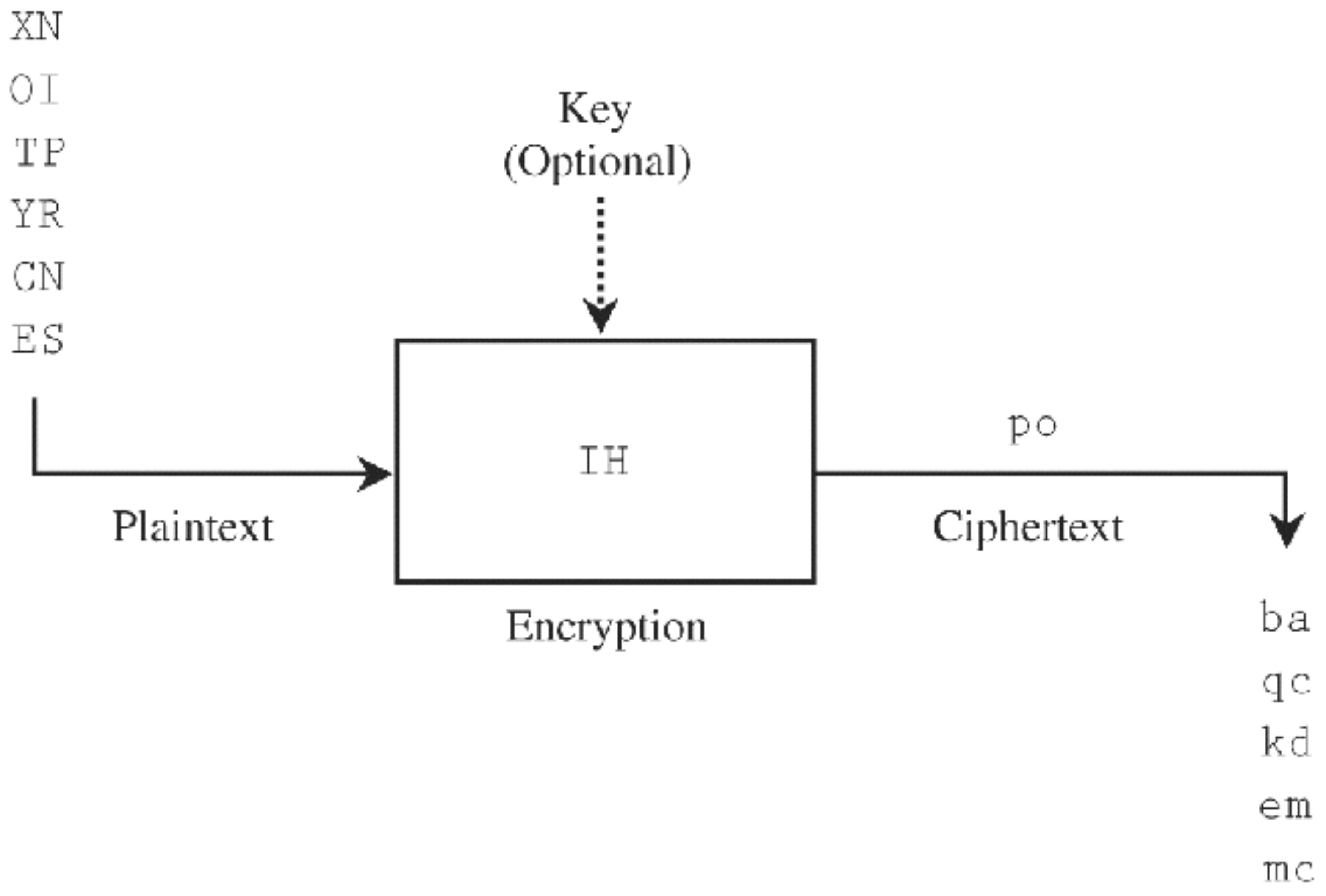


Vernam Cipher

mind you, this is potentially unbreakable!! yet…

stream vs block ciphers





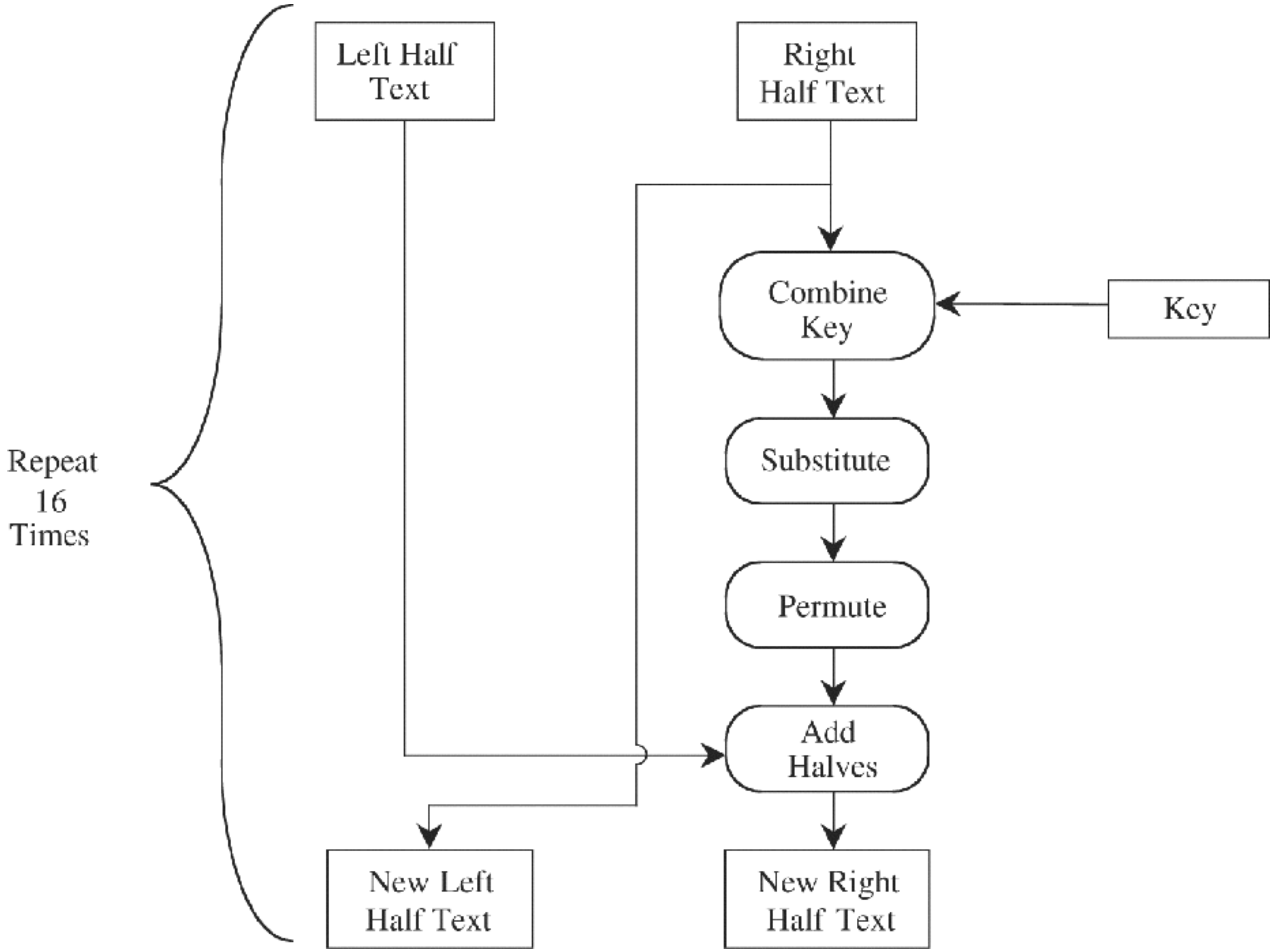
Stream Encryption

speed

Block Cipher Systems

diffusion

basic scheme of des (and 3des)

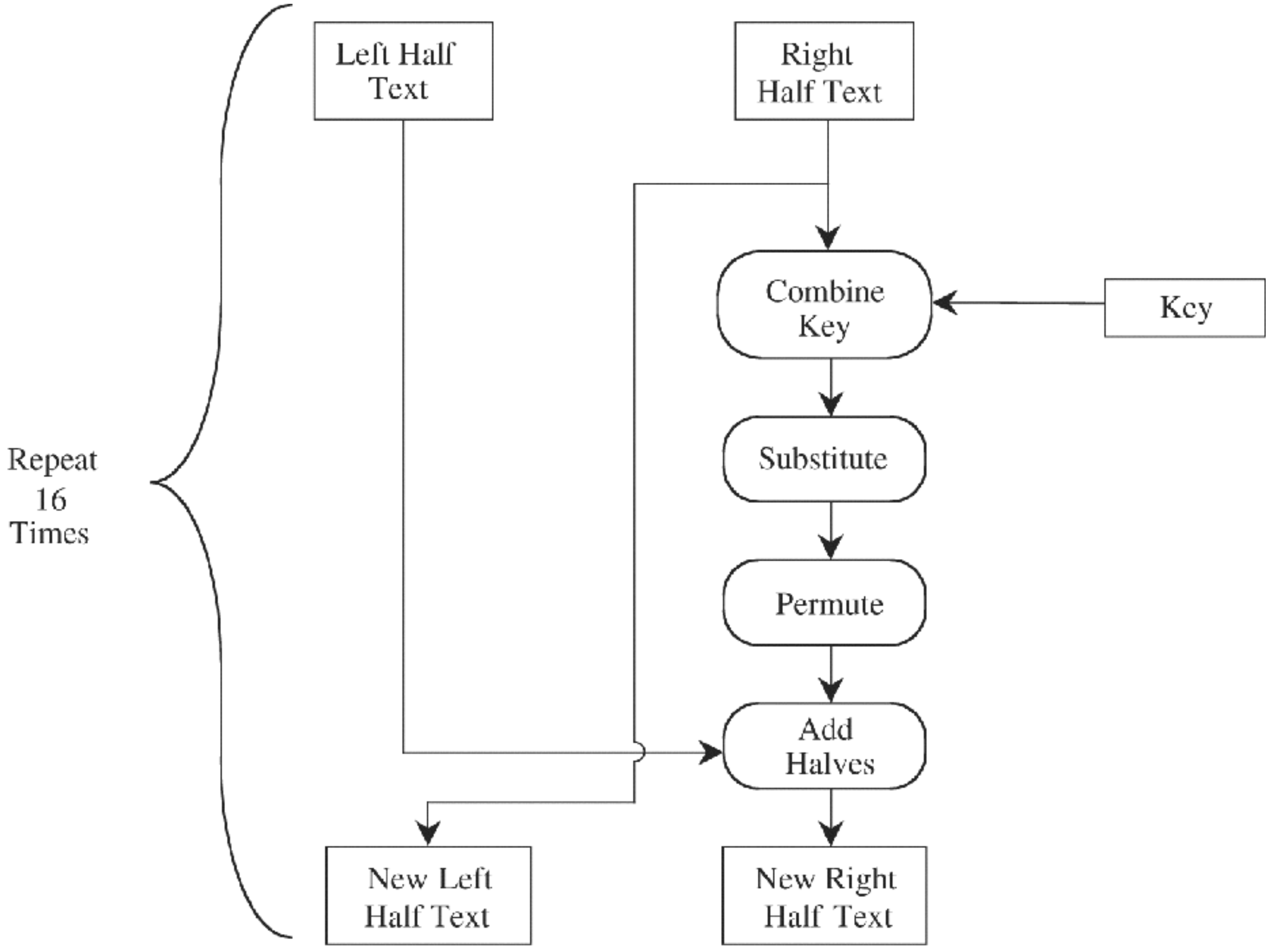


confusion

diffusion

Cycles of Substitution and Permutation

basic scheme of des (and 3des)



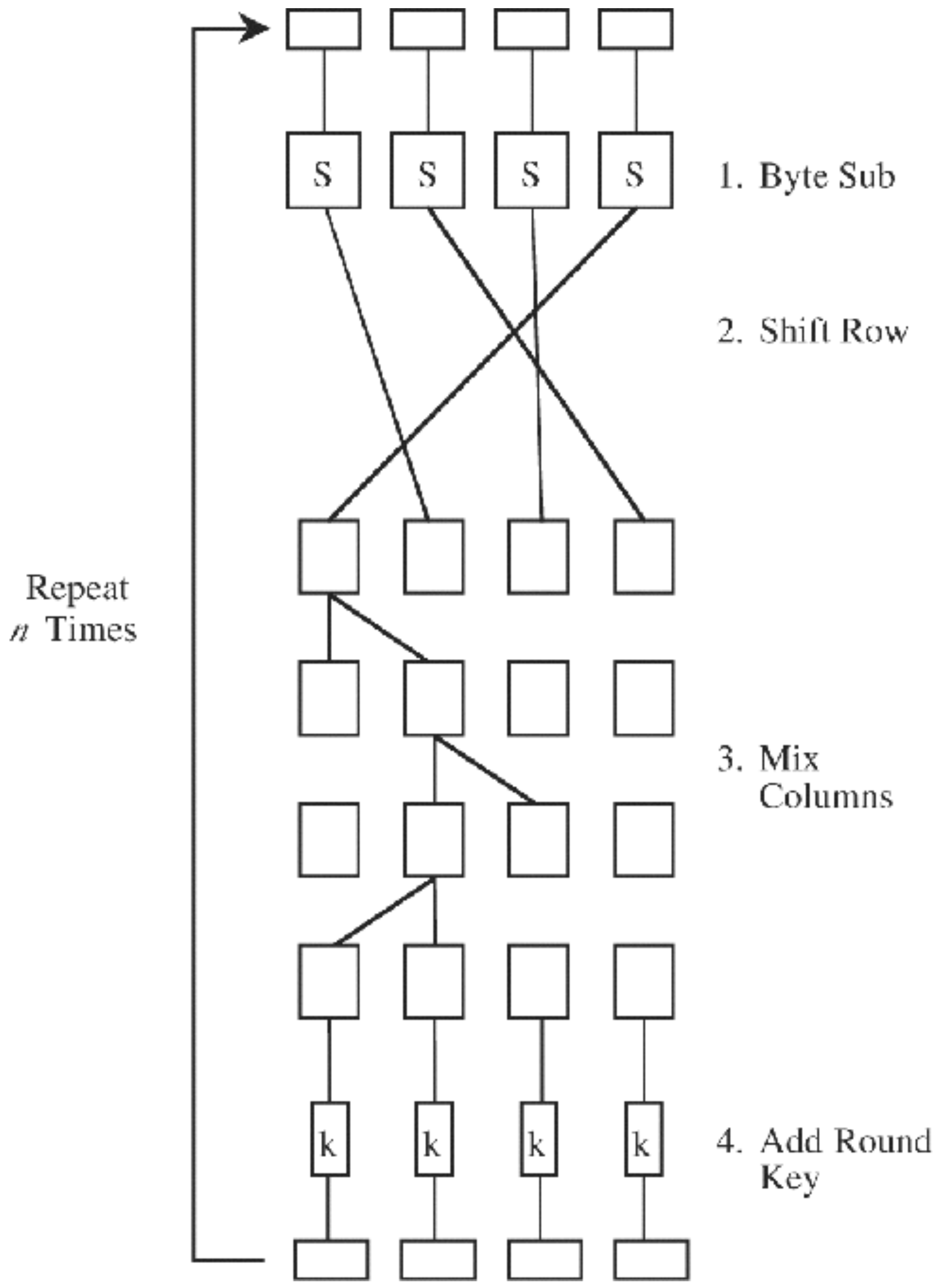
confusion

diffusion

56bit encryption
not good enough

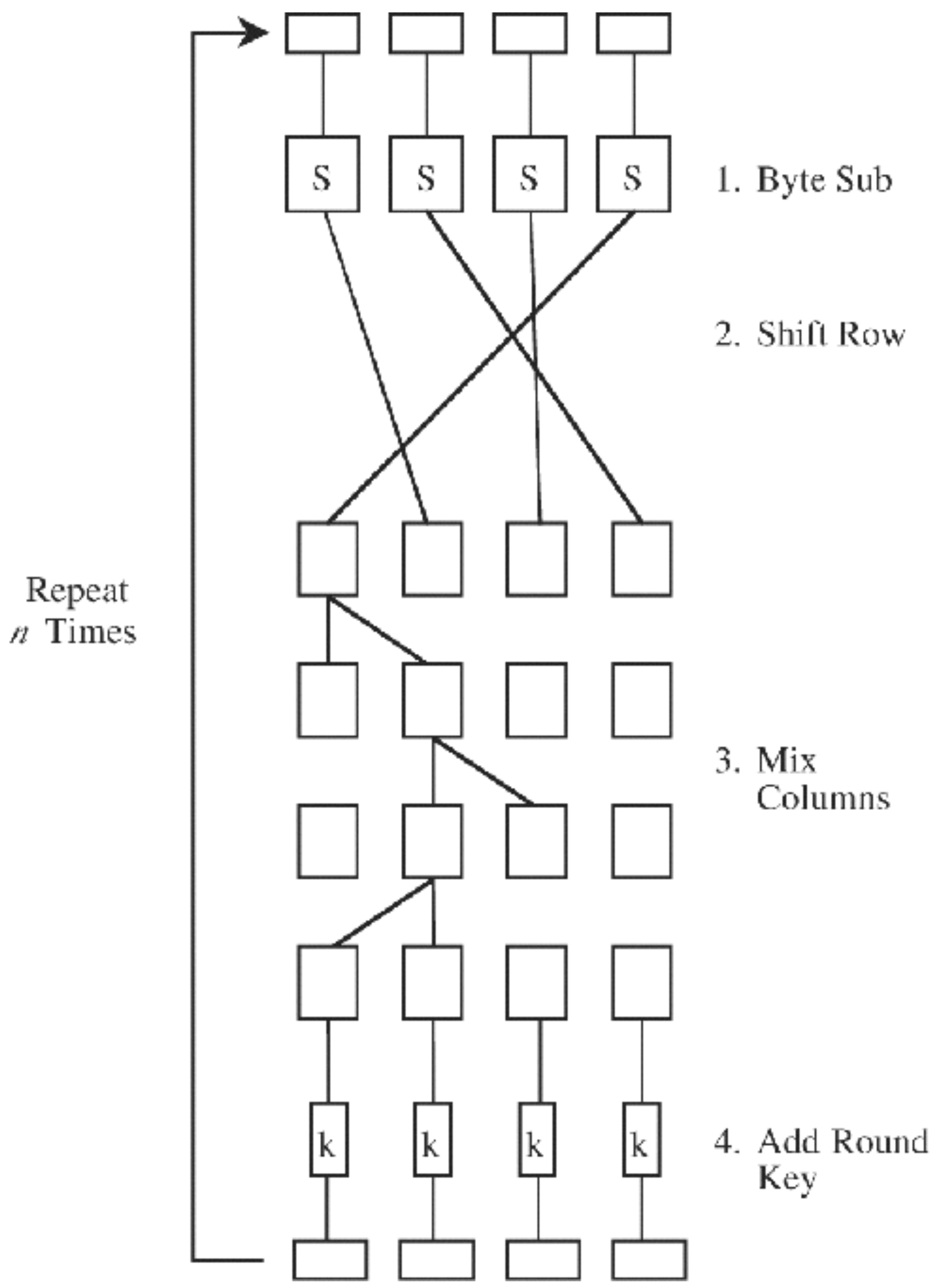
Cycles of Substitution and Permutation

basic scheme of aes

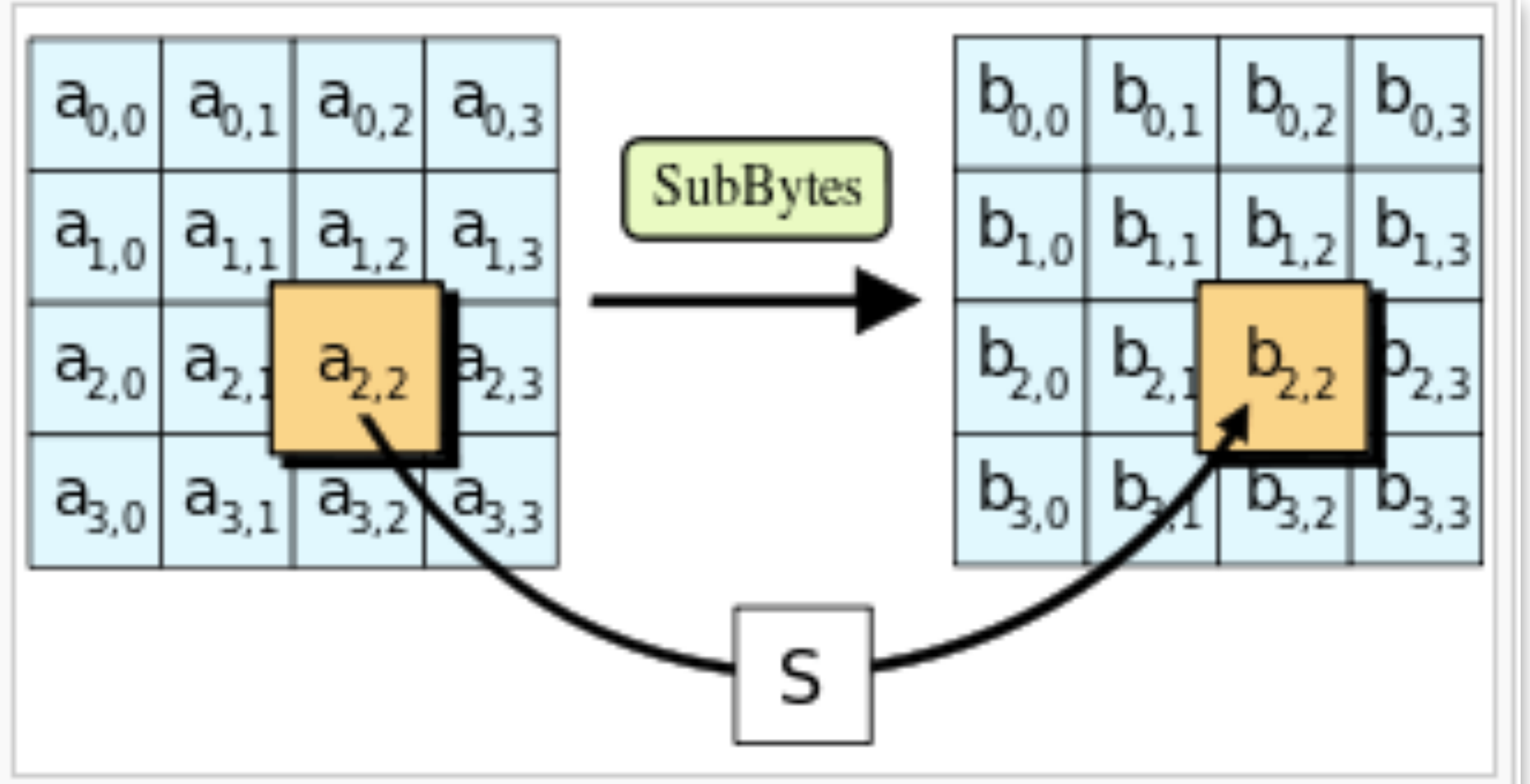


AES Algorithm

basic scheme of aes

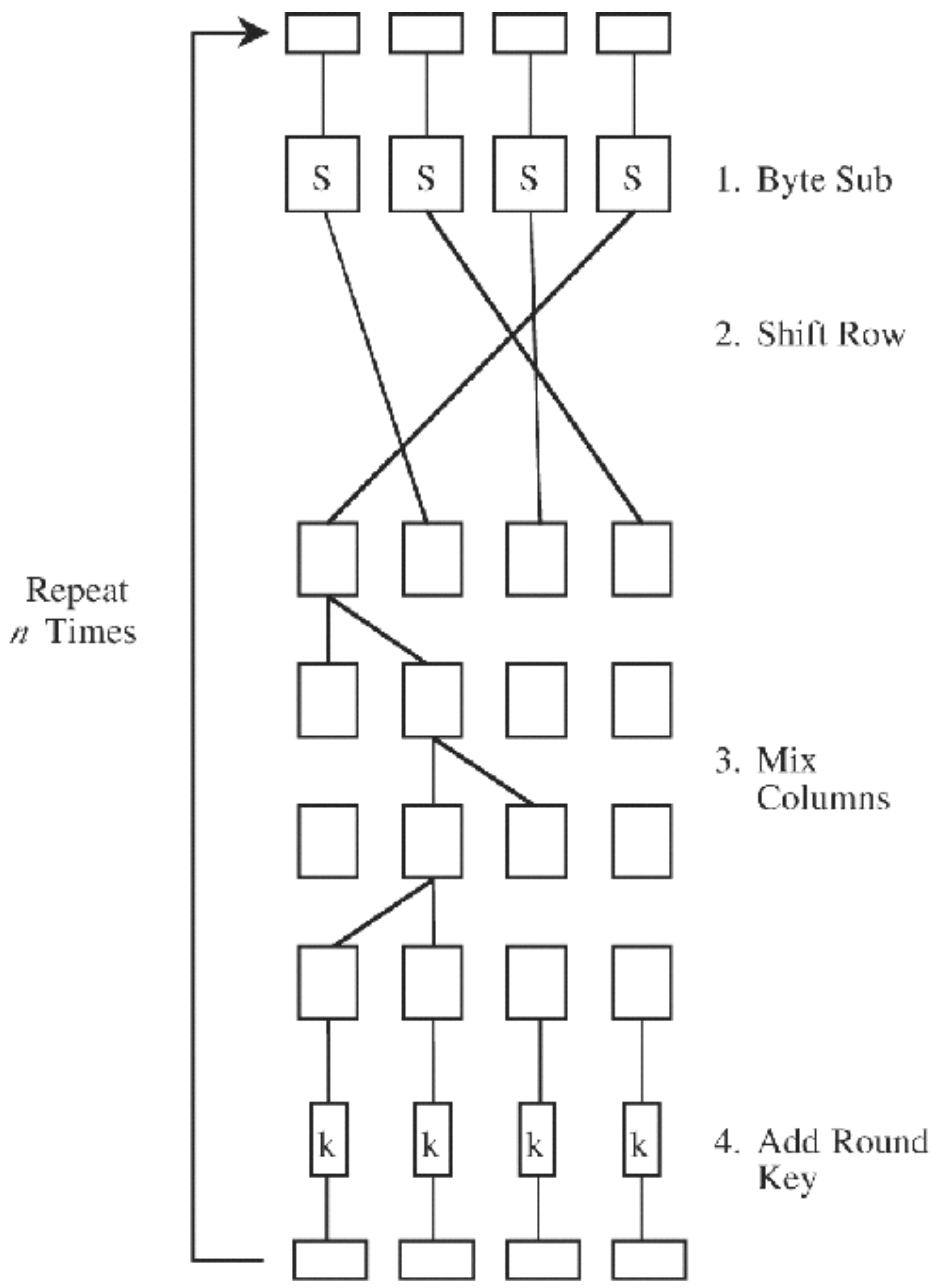


AES Algorithm

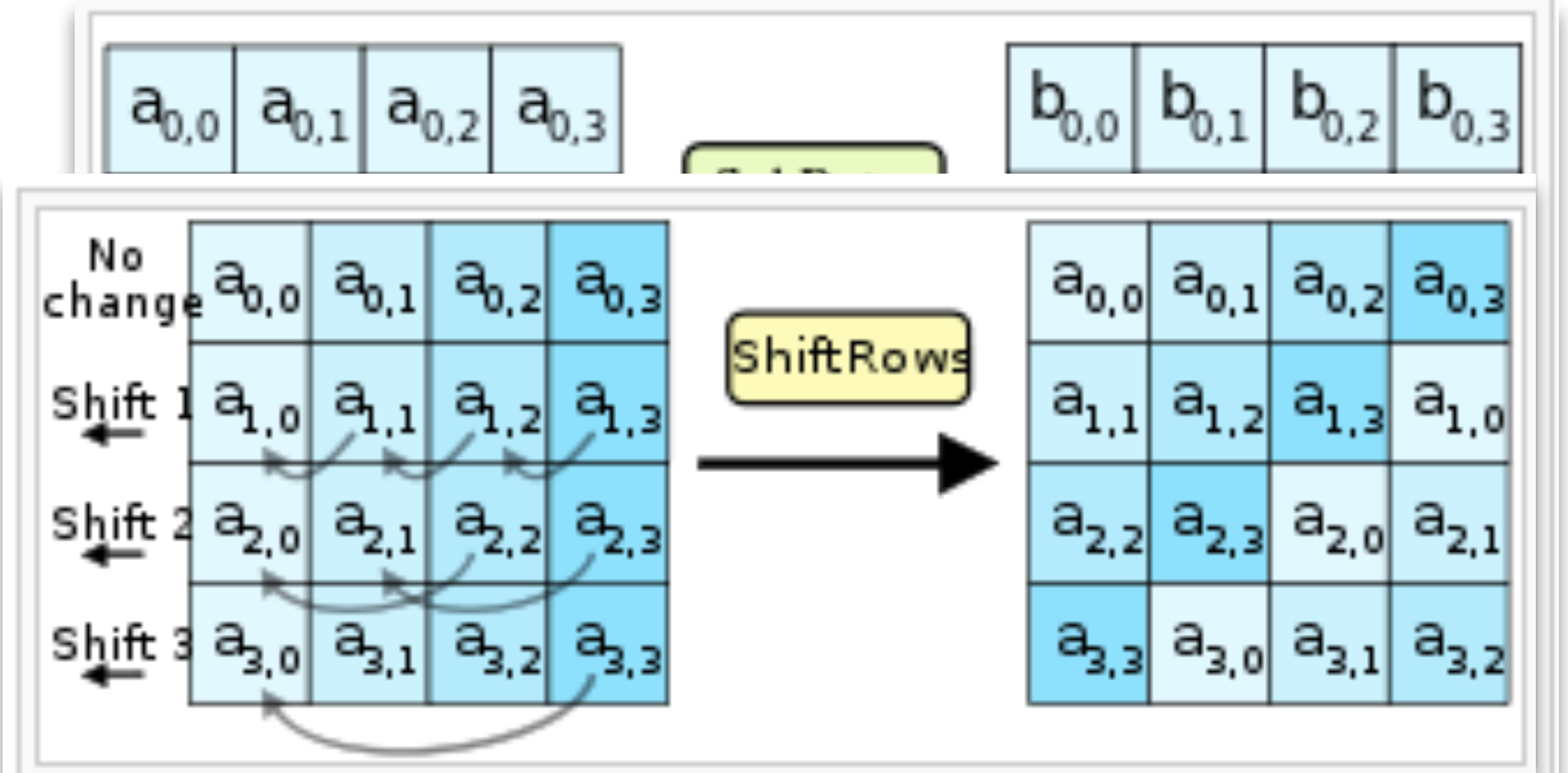


In the `SubBytes` step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, *S*; $b_{ij} = S(a_{ij})$.

basic scheme of aes

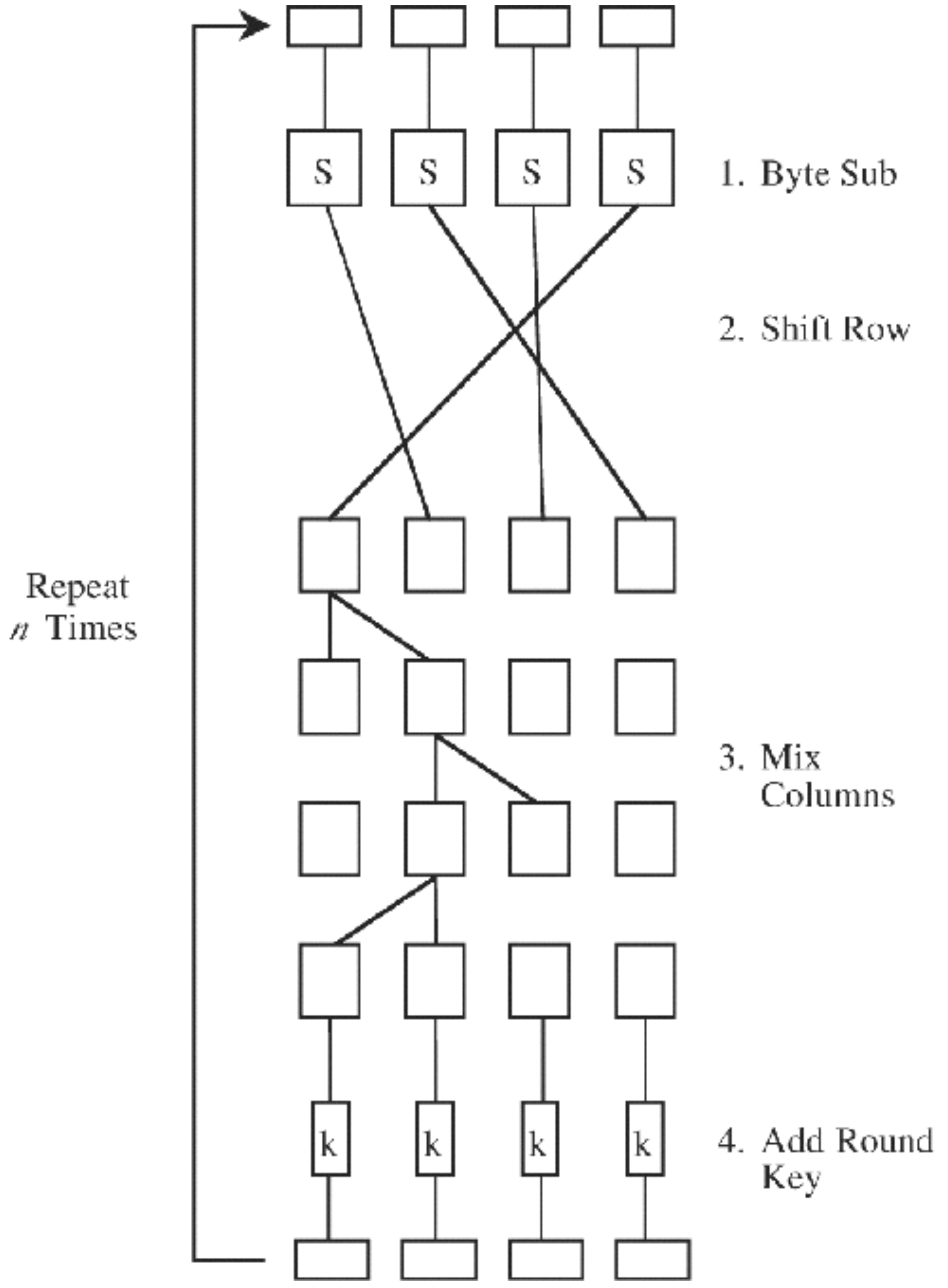


AES Algorithm

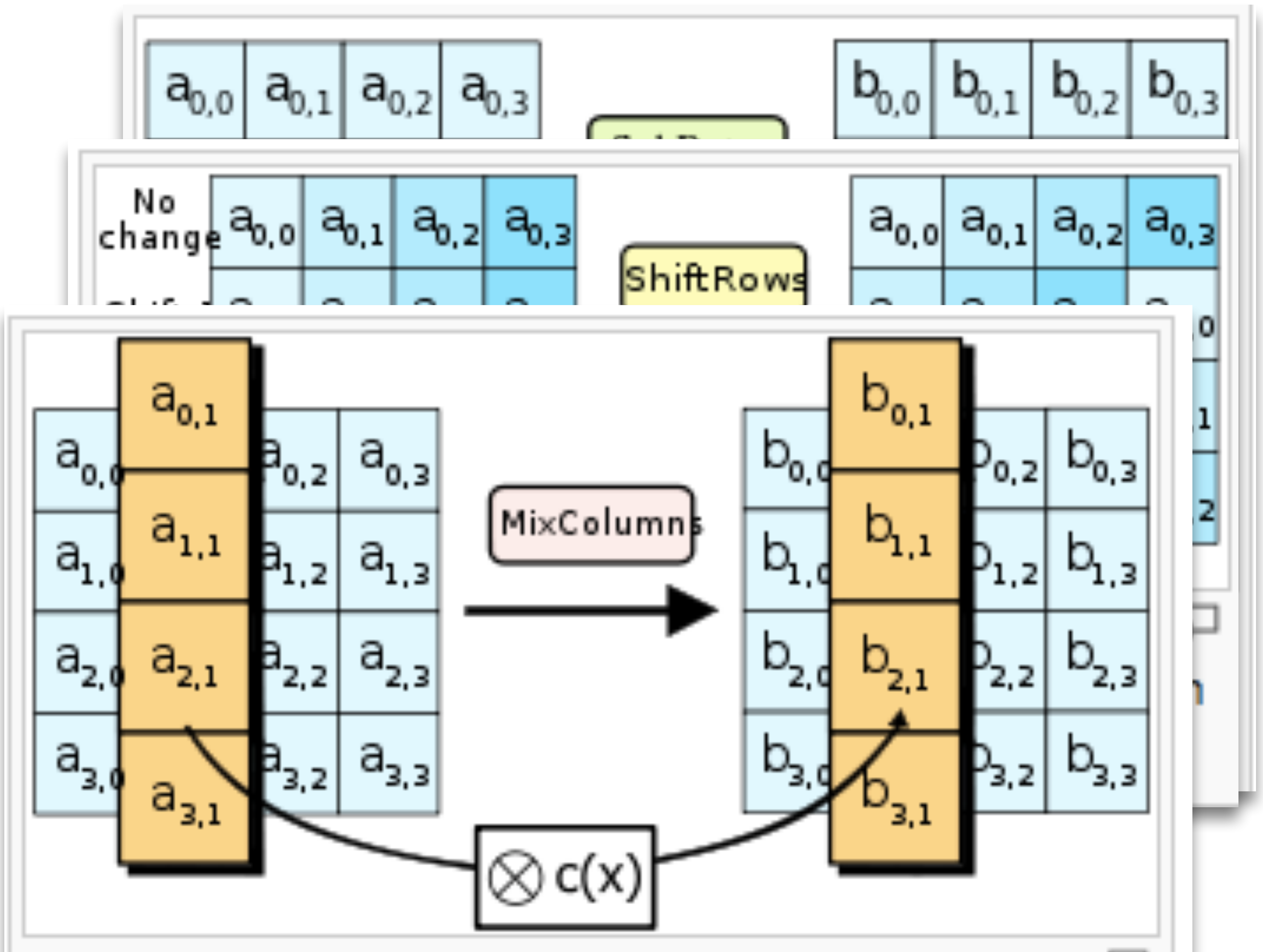


In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

basic scheme of aes

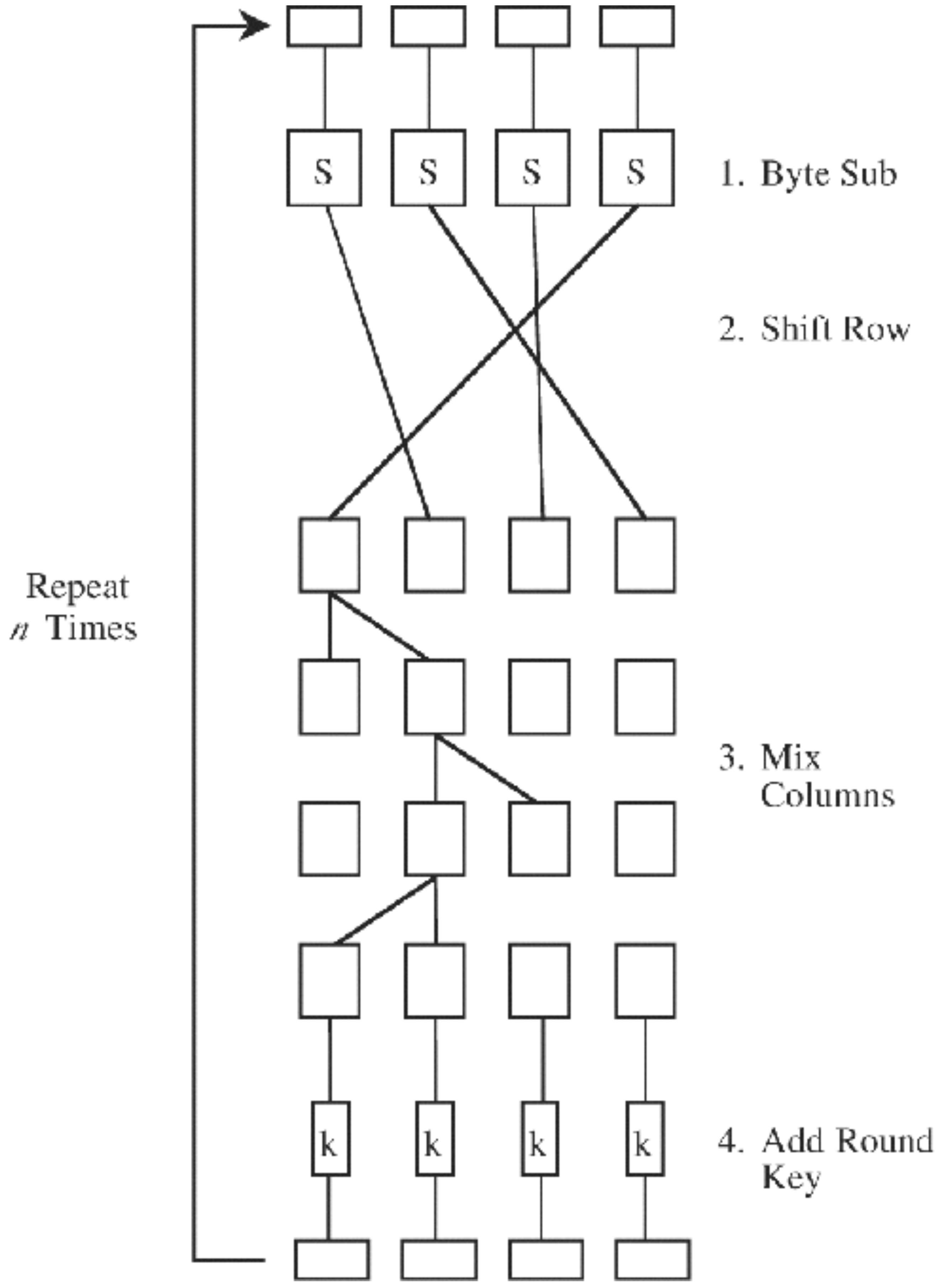


AES Algorithm

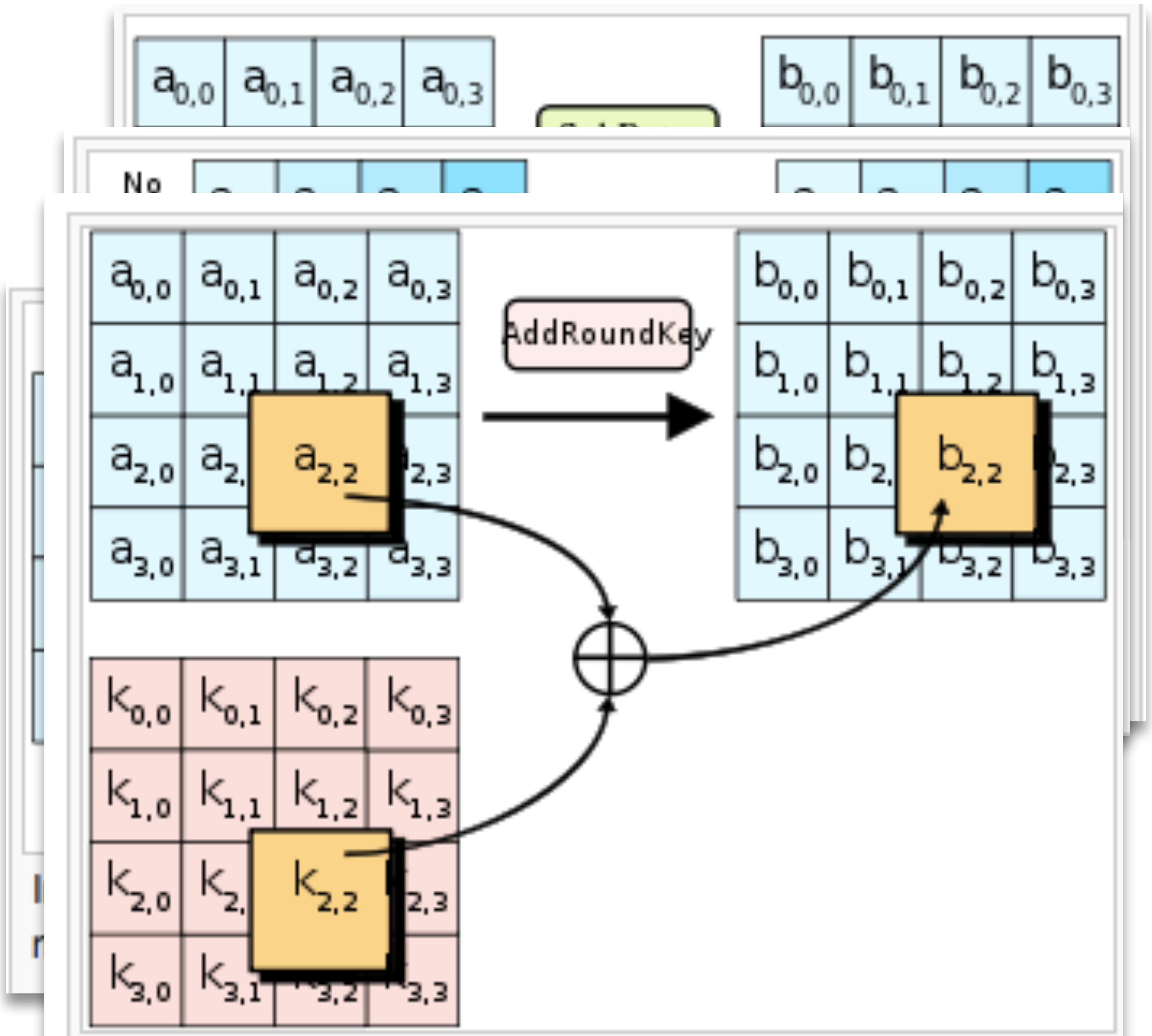


In the MixColumns step, each column of the state is multiplied with a fixed polynomial *c(x)*.

basic scheme of aes



AES Algorithm



In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation (⊕).

comparison

TABLE 2-4 Comparison of DES and AES.

	DES	AES
Date	1976	1999
Block size	64 bits	128 bits
Key length	56 bits (effective length)	128, 192, 256 (and possibly more) bits
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accepted open public comment
Source	IBM, enhanced by NSA	Independent Dutch cryptographers

Topics in lecture

Primary network security issues

Cryptographic fundamentals

- Symmetric/asymmetric encryption
- **Digital Signatures,** Certificates and PKI

Two well known security protocols

Digital signatures

Most common use for asymmetric encryption

Piece of data attached to a message to guarantee integrity

Involves the use of digests and hashing functions

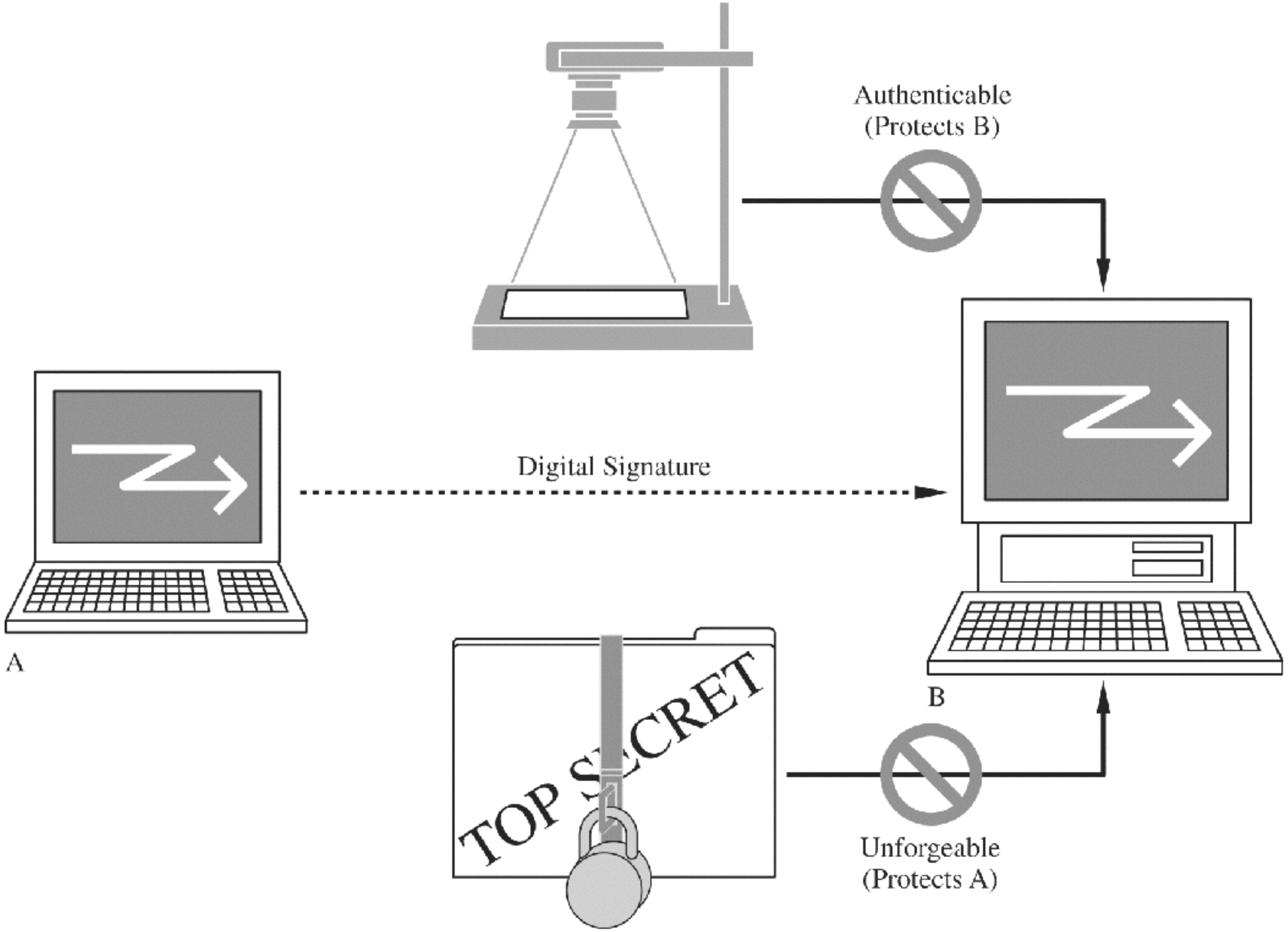
- A hashing function takes data as input and produces a smaller piece of data (digest) as output
- If original input data changes even ***slightly***, digest is ***very*** different; computationally unfeasible to create text to obtain given hash

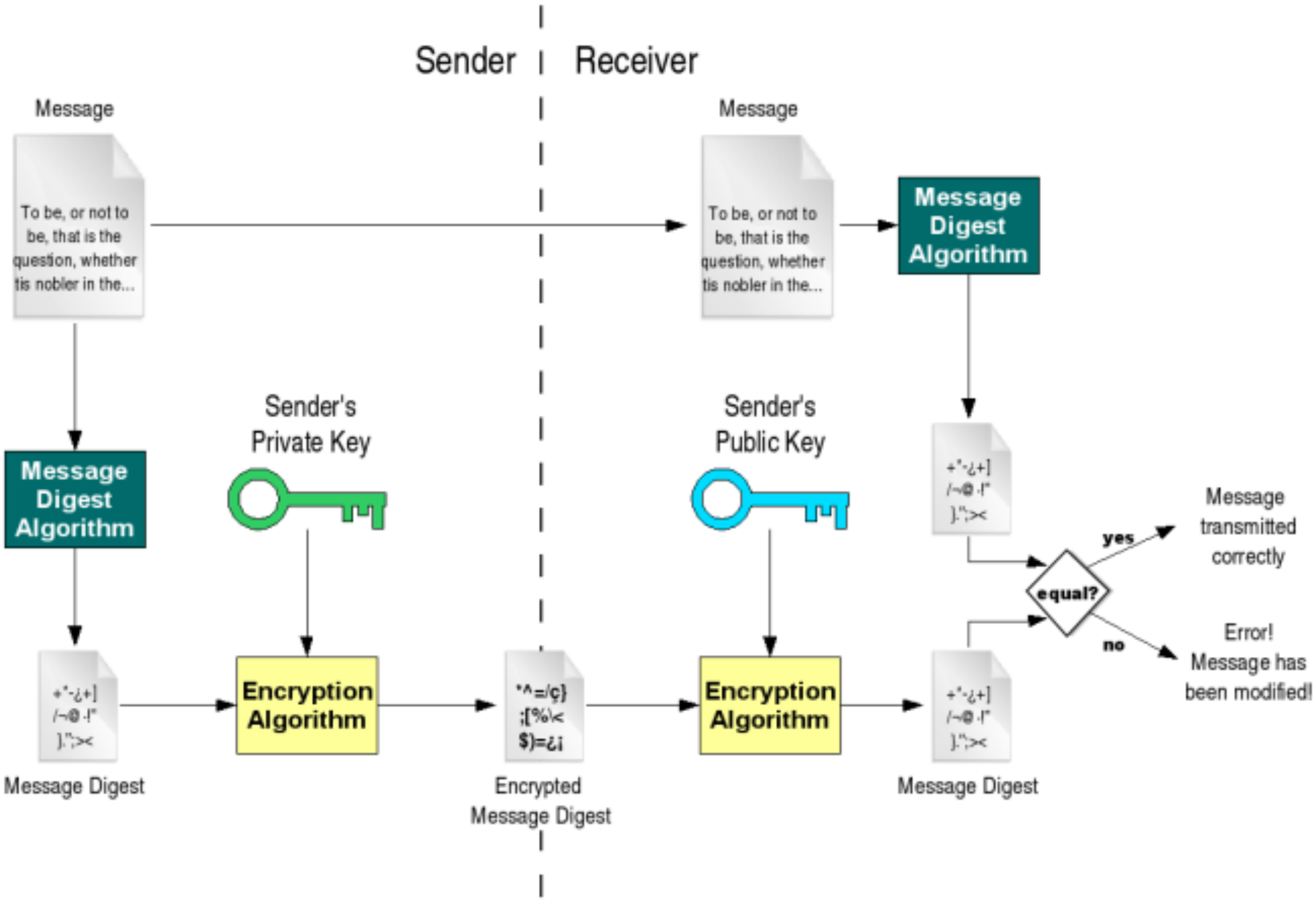
Assurances:

- Message had been created/accessed by the holder of the private key (***authentication***)
- Holder of private key cannot deny having created/accessed the message which has been signed (***non-repudiation***)
- Message has not been tampered with (***integrity***)
- Does not provide confidentiality as message is sent in the clear

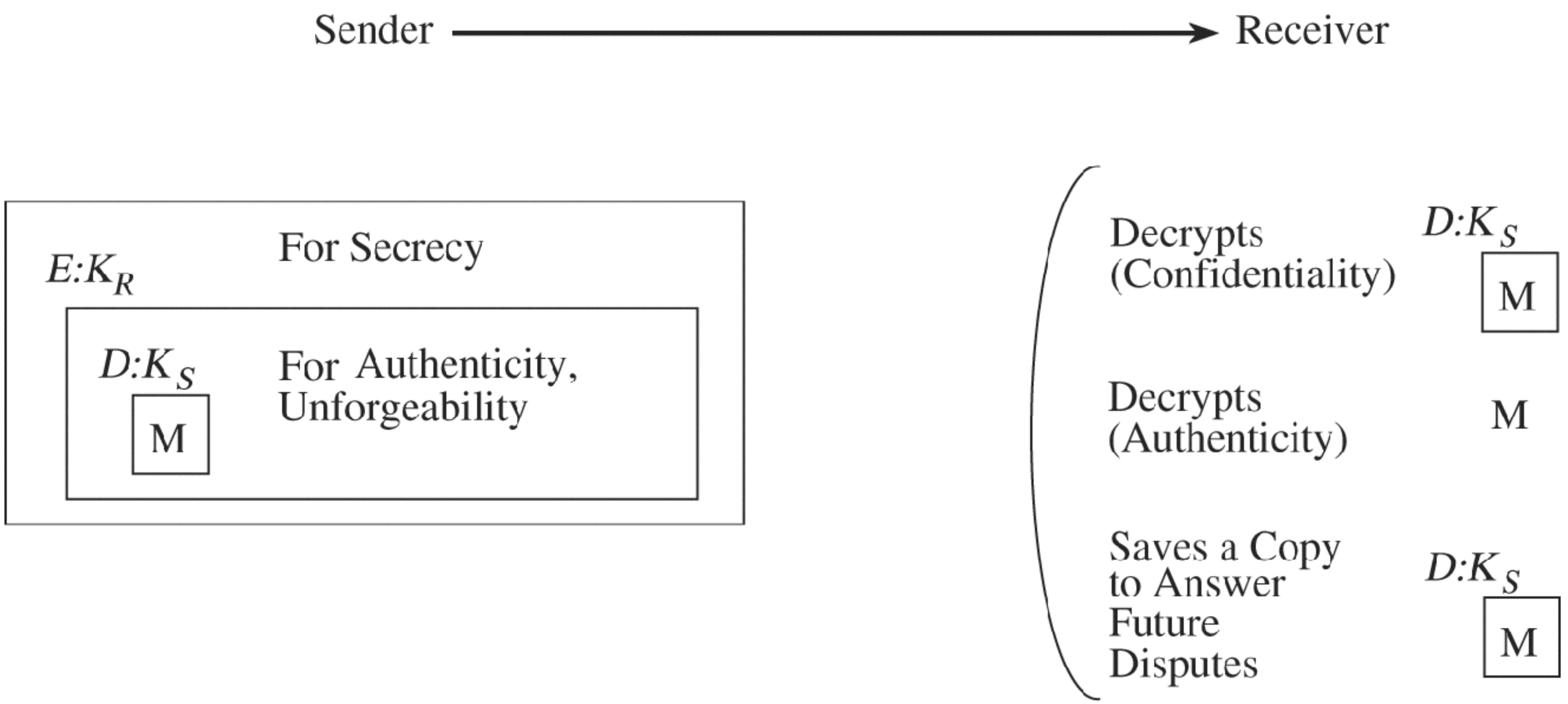
Example algorithms: RSA, DSA, ECDSA

Requirements for a Digital Signature




Sender
Receiver
Message
To be, or not to be, that is the question, whether tis nobler in the...
Message
To be, or not to be, that is the question, whether tis nobler in the...
Message Digest Algorithm
Sender's Private Key
Sender's Public Key
Message Digest Algorithm
yes
Message transmitted correctly
equal?
no
Error! Message has been modified!
Encryption Algorithm
Encryption Algorithm
Message Digest
Encrypted Message Digest
Message Digest

Keys in Asymmetric Digital Signature



Topics in lecture

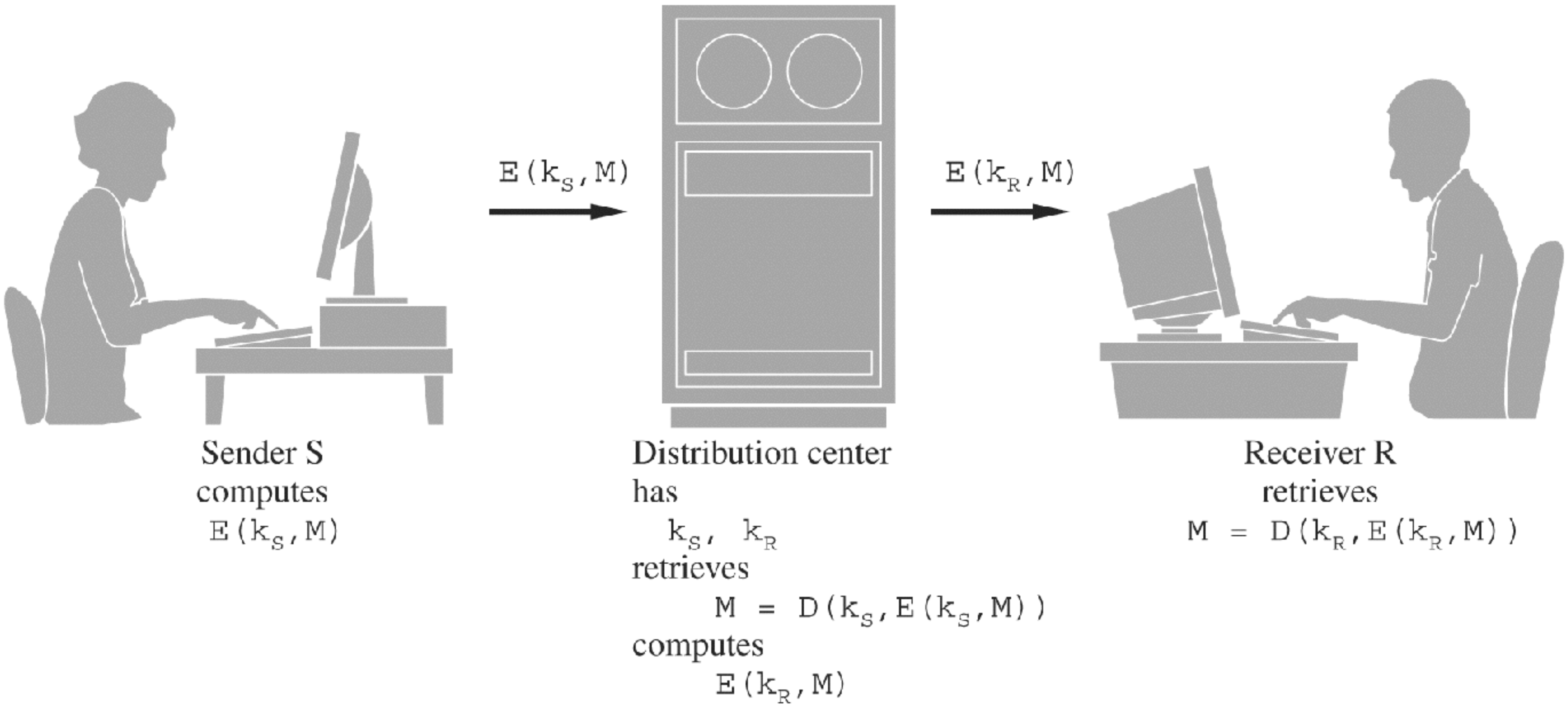
Primary network security issues

Cryptographic fundamentals

- Symmetric/asymmetric encryption
- Digital Signatures, **Certificates and PKI**

Two well known security protocols

the problem of key distribution



how to exchange keys so that nobody else can obtain a copy?

the problem of key distribution

in principle the problem goes away with PK crypto.

In fact, it was the main driver of PK crypto. Yet…

identification: how to ensure a PKey belongs to its owner?

Public Key Infrastructure, Web of Trust, …

key exchange: can we exchange symmetric keys securely?

Diffie-Hellman protocol, Quantum key exchange

Certificates and Certificate Authorities

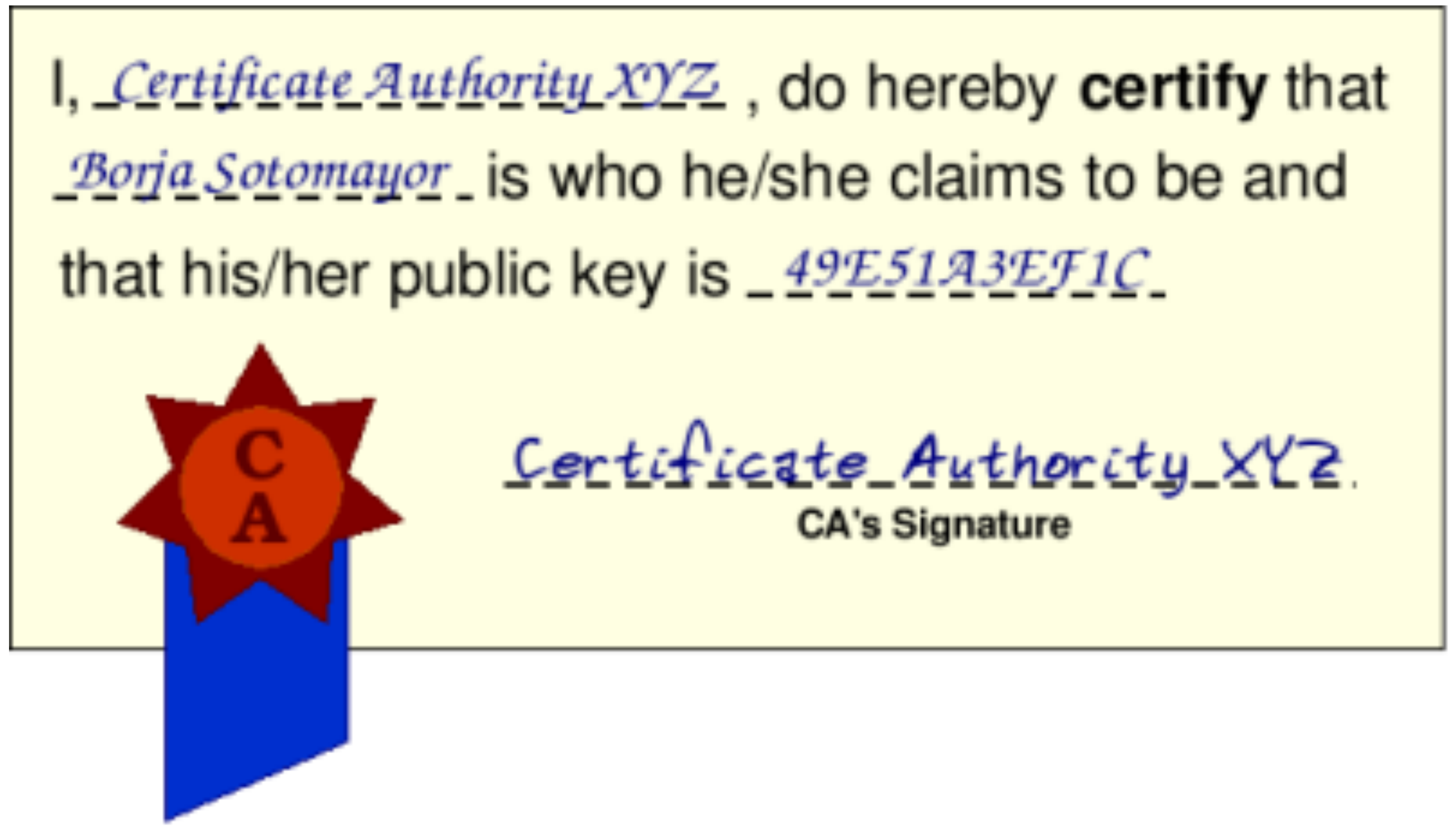
For authentication, need to guarantee public key corresponds to correct private key

Certificate is a digital document that certifies a public key belongs to a specific user with an identity

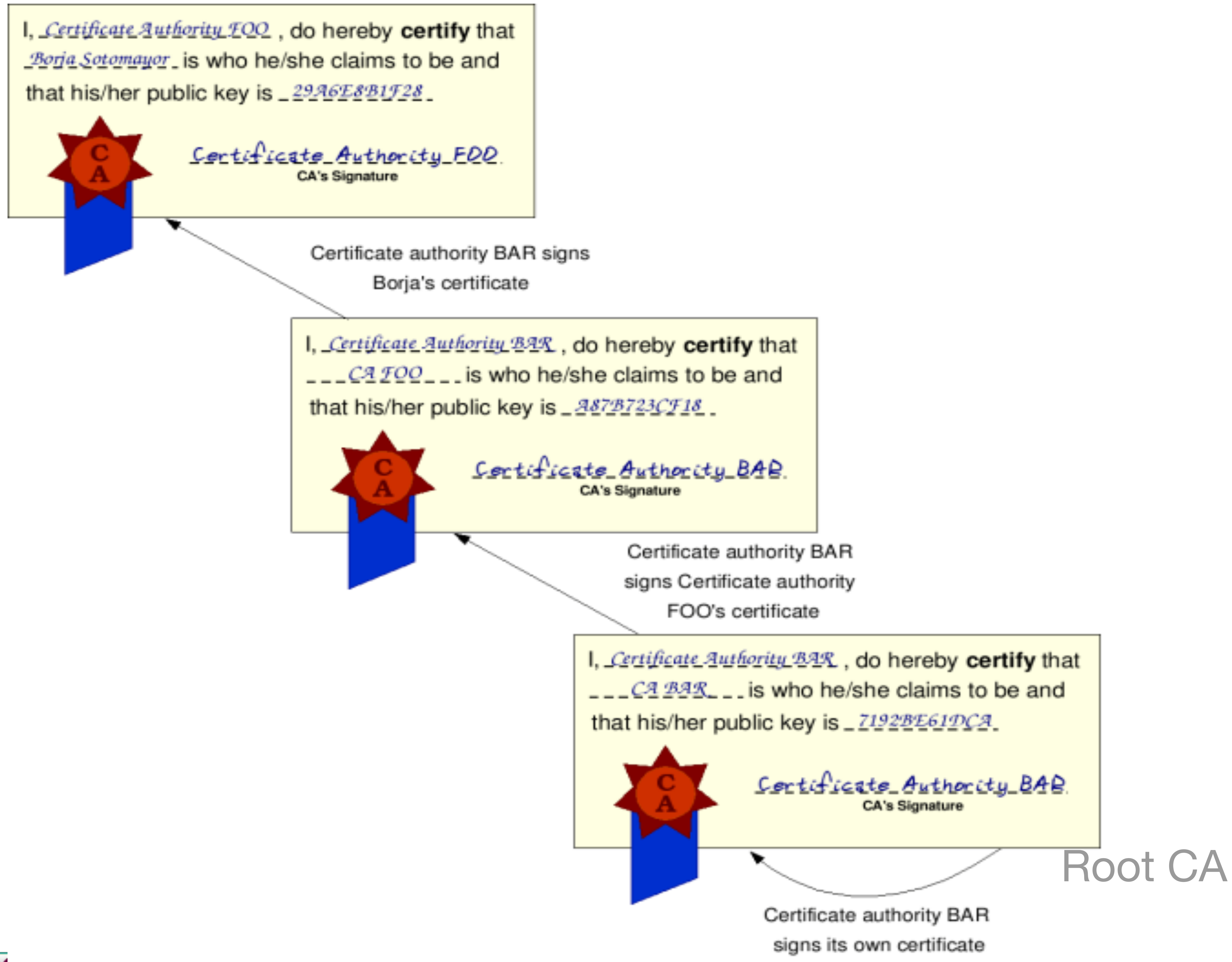
Certificate is signed by a trusted third party – Certificate Authority (CA) with its private key

Public key of CA distributed widely in standard applications (e.g. Web browsers)

Well known CAs: Verisign, Thawte, GlobalSign, Comodo, …


I, Certificate Authority XYZ , do hereby certify that
Borja Sotomayor is who he/she claims to be and
that his/her public key is 49E51A3EF1C
C A
Certificate Authority XYZ
CA's Signature

Hierarchy of CAs



Public Key Infrastructure (PKI)

Infrastructure through which certificates are managed

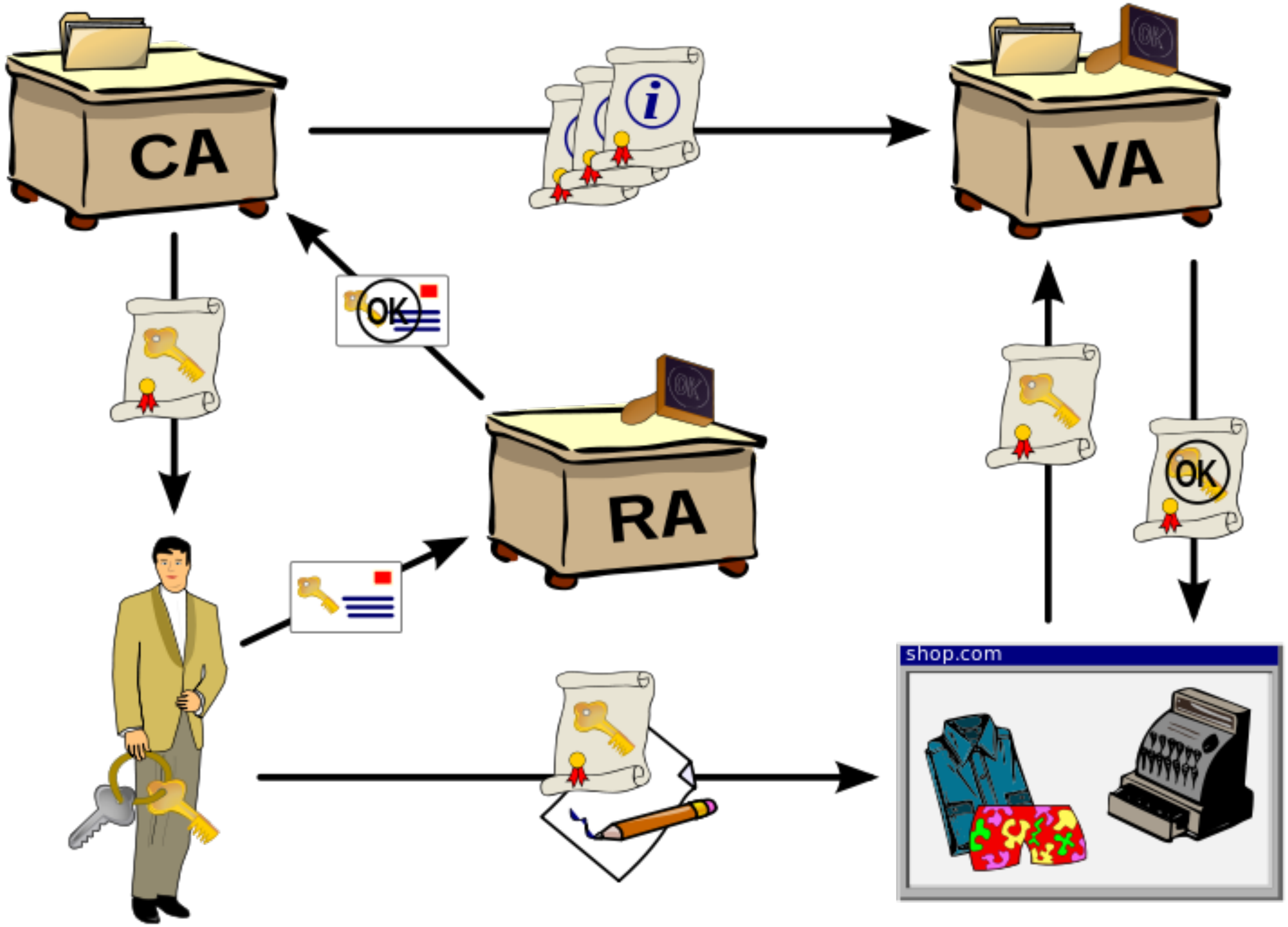
Involves:

- Generation of new certificates and private keys
- Storage of certificates
- Distribution / Revocation / Archival

Widely used standard for certificates in PKI: X509v3

- User identities are represented as Distinguished Names (DNs)
- These include: Organization (O), Organizational Unit (OU), Common Name (CN), Country (C)
- Example: O=University of Southampton, OU=Department of Electronics and Computer Science, CN=Mr Anderson

Public Key Infrastructure (PKI)



Alternative approaches to keys

Web of trust

Self-signed certificates: PGP, GnuPG

Simple Public Key Infrastrustrucre (SPKI)

the *key* is trusted, not the person;
no personal authentication

No notion of trust: verifier is also the issuer.

A coffer analogy…

A coffer analogy…

A paint analogy…

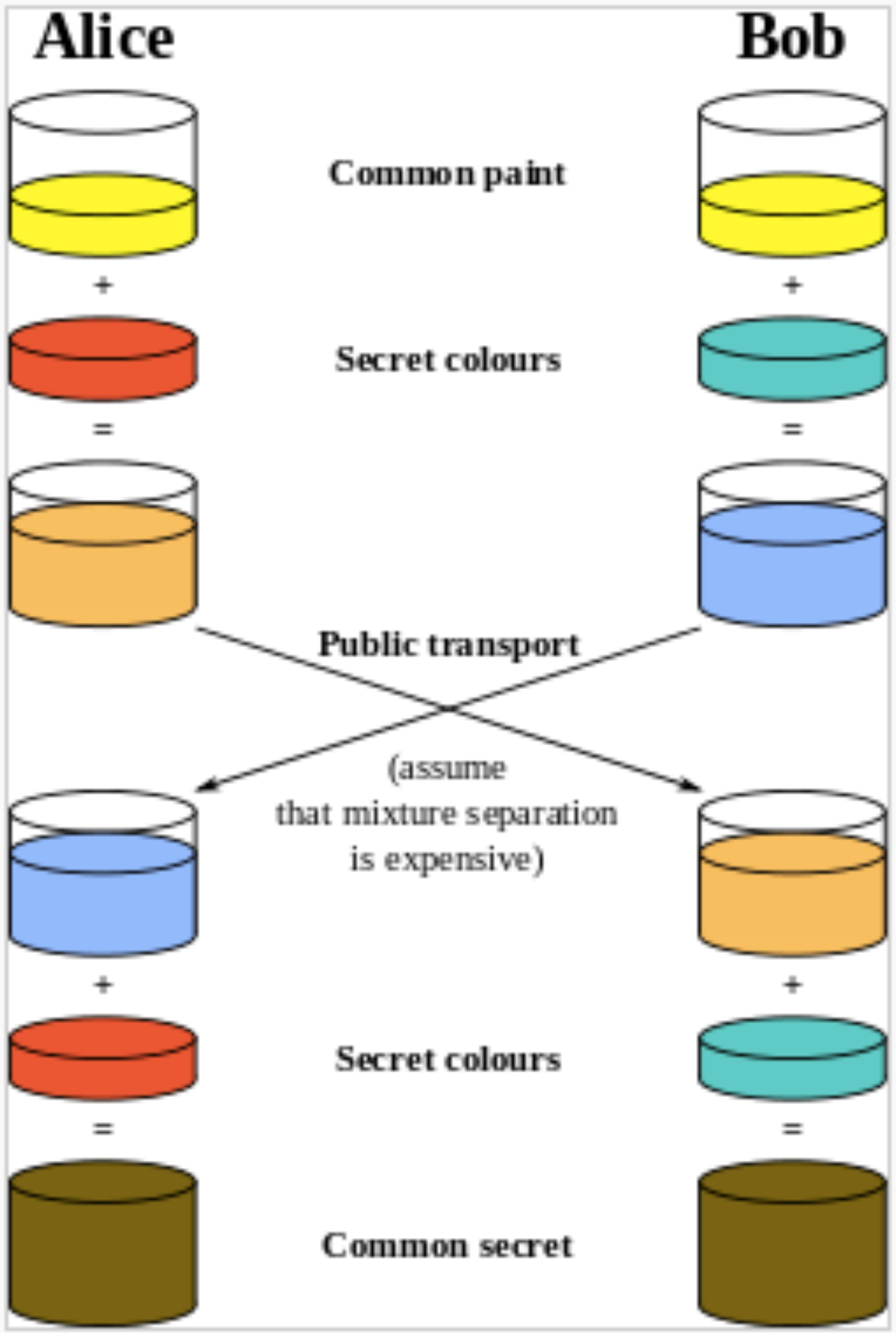


Illustration of the Diffie–Hellman Key Exchange

In pratice:

1. Alice and Bob agree to use a prime number $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $a = 6$, then sends Bob $A = g^a \bmod p$
   - $A = 5^6 \bmod 23 = 8$
3. Bob chooses a secret integer $b = 15$, then sends Alice $B = g^b \bmod p$
   - $B = 5^{15} \bmod 23 = 19$
4. Alice computes $s = B^a \bmod p$
   - $s = 19^6 \bmod 23 = 2$
5. Bob computes $s = A^b \bmod p$
   - $s = 8^{15} \bmod 23 = 2$
6. Alice and Bob now share a secret (the number 2).

University of Southampton

In pratice:

Alice	
knows	doesn't know
$p = 23$	$b = ?$
base $g = 5$	
$a = 6$	
$A = 5^a \bmod 23$	
$A = 5^6 \bmod 23 = 8$	
$B = 19$	
$s = B^a \bmod 23$	
$s = 19^6 \bmod 23 = 2$	
$s = 2$	

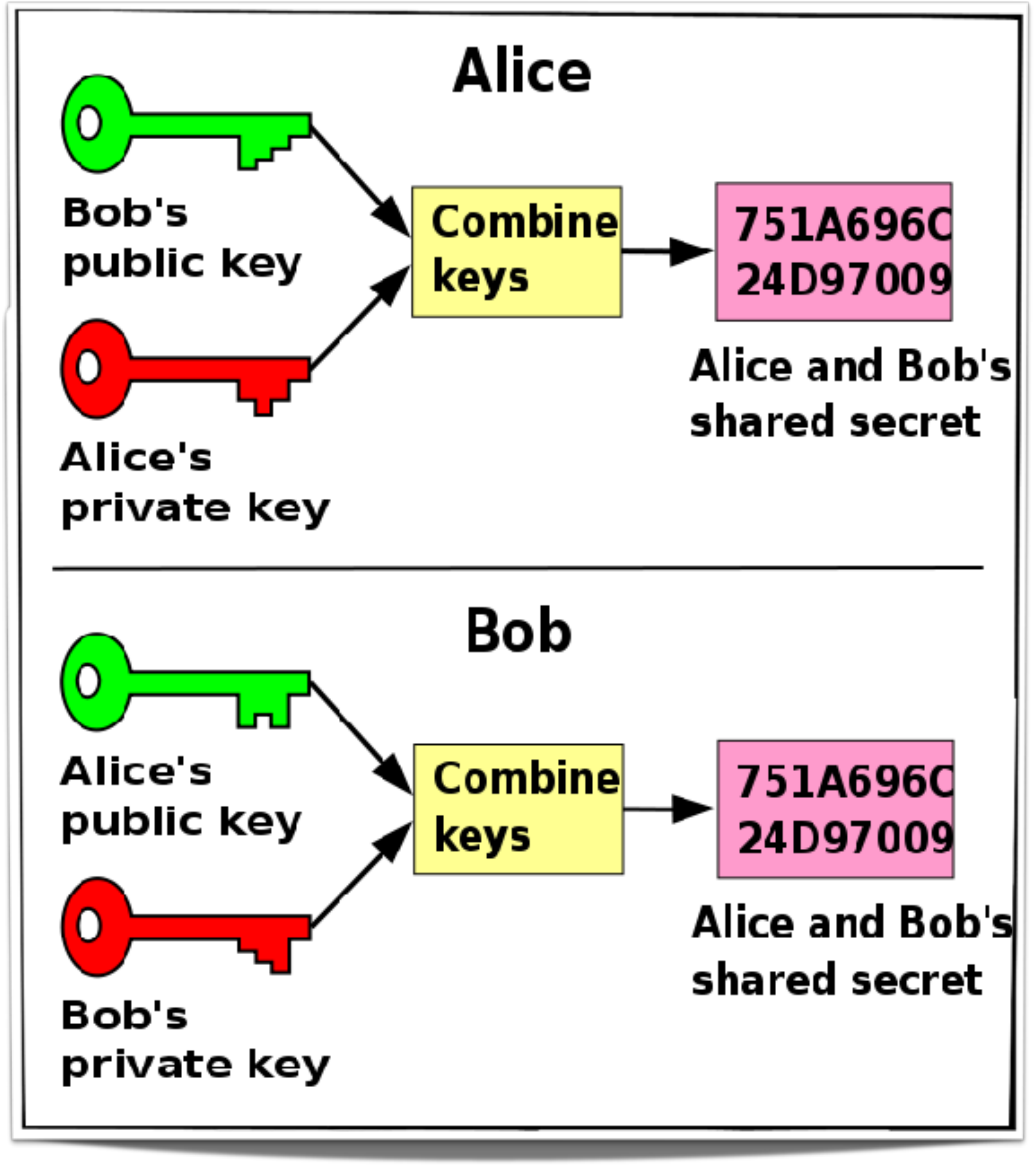
Bob	
knows	doesn't know
$p = 23$	$a = ?$
base $g = 5$	
$b = 15$	
$B = 5^b \bmod 23$	
$B = 5^{15} \bmod 23 = 19$	
$A = 8$	
$s = A^b \bmod 23$	
$s = 8^{15} \bmod 23 = 2$	
$s = 2$	

Eve	
knows	doesn't know
$p = 23$	$a = ?$
base $g = 5$	$b = ?$
	$s = ?$
$A = 8$	
$B = 19$	
$s = 19^a \bmod 23 = 8^b \bmod 23$	

- Now s = the shared secret key and it is known to both Alice and Bob, but *not* to Eve. $s = 2$

University of Southampton

A posteriori explanation:



but this protocol predates PK crypto

Alice transmits random bits as polarised photons according to a randomly selected basis + or x

Basis	0	1
+	↑	→
×	↗	↘

Only by randomly selecting the same basis can Bob be sure of the measurement

Alice's random byte	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→

Basis	0	1
+	↑	→
×	↗	↘

Alice and Bob compare the basis for each photon over public classic channel, throw away bits were they differ

They also compare a sample of the remaining bits: if Eve has intercepted them, they'll differ, and so…

Alice's random byte	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→

Topics in lecture

Primary network security issues

Cryptographic fundamentals

Two well known security protocols

- **SSL**
- Kerberos

SSL

Most widely known protocol for securing client-server communication on the Internet (transport layer)

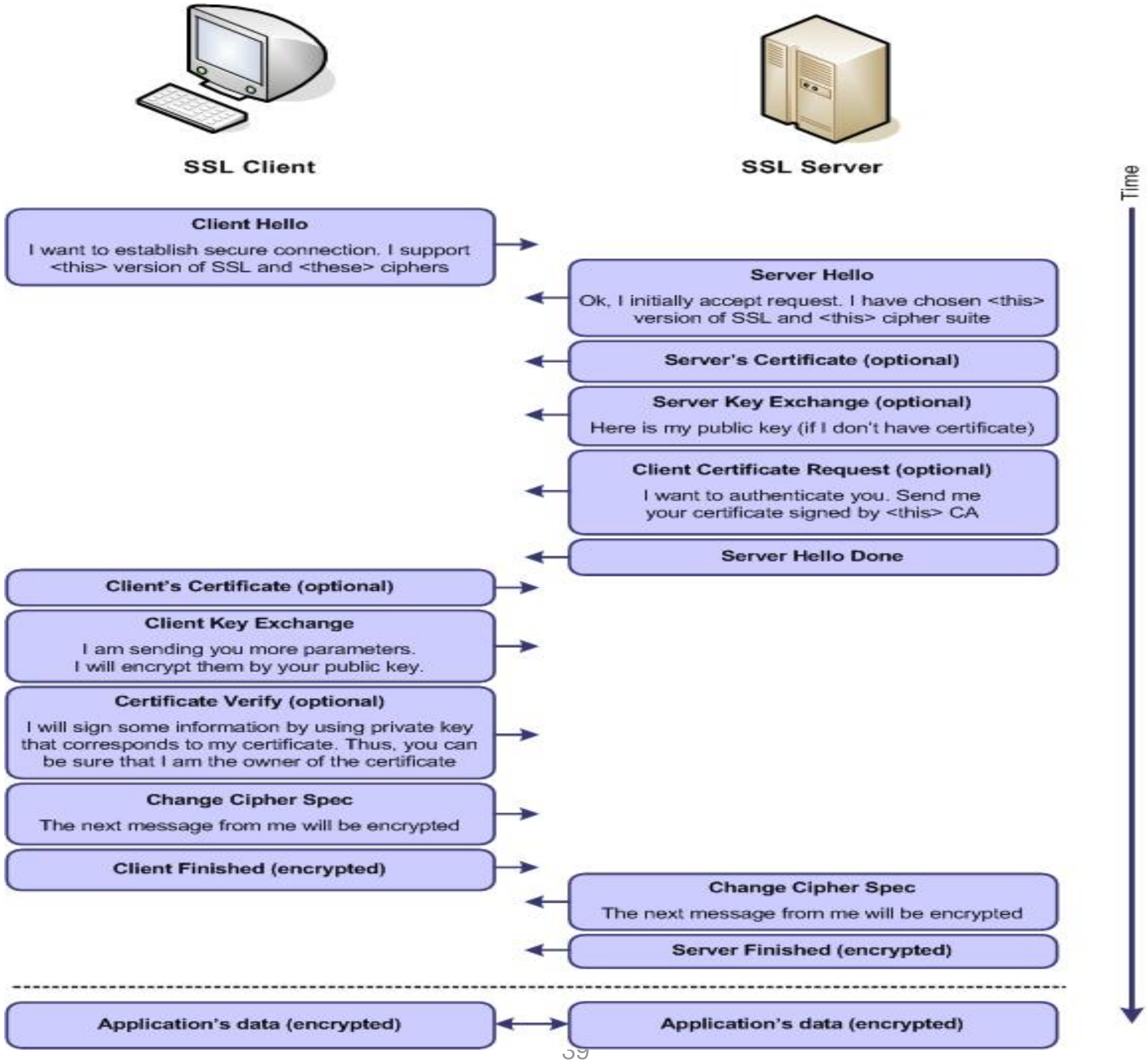
Used to establish an encrypted tunnel to secure protocols like HTTP

Optional mutual authentication through certificates

Common versions: SSLv3 and TLS

Based on X509v3 certificates

SSL Security Handshake



Topics in lecture

- Primary network security issues
- Cryptographic fundamentals
- **Two well known security protocols**
  - SSL
  - **Kerberos**

Kerberos

Popular protocol for authenticating users in a networked environment (e.g. Windows NT, 2000, Server)

Based on symmetric encryption for faster performance

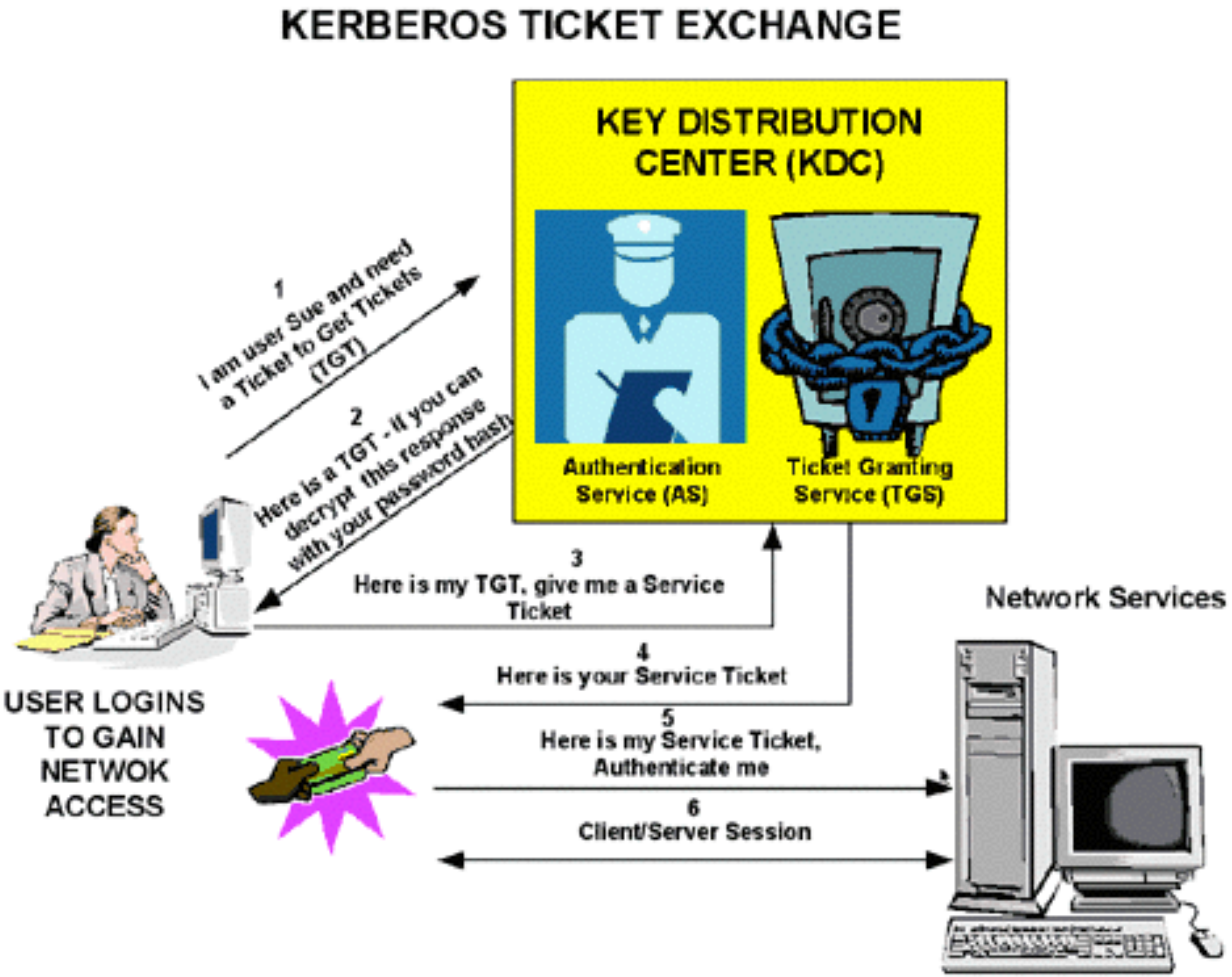
Every host on the network has its own secret key, which is known to a central server (Key Distribution Center)

Session keys are generated for communication between client and KDC / server

User provides an ID (username)/password once to obtain a Ticket Granting Ticket (TGT)

TGT can be used to obtain access various resources on application servers through various service tickets issued by the Ticket Granting Service (TGS)

Kerberos protocol



Methods of authentication

Username/password

- HTTP Basic Auth – protocol between a Web browser and server with username/password encoded into HTTP header
- Password usually protected using SSL (https)

Kerberos

- Using session keys and service tickets
- Faster – based on secret keys, no non-repudiation

PKI and X509 certificates

- Using signatures attached to messages
- Also provides non-repudiation, integrity but slower