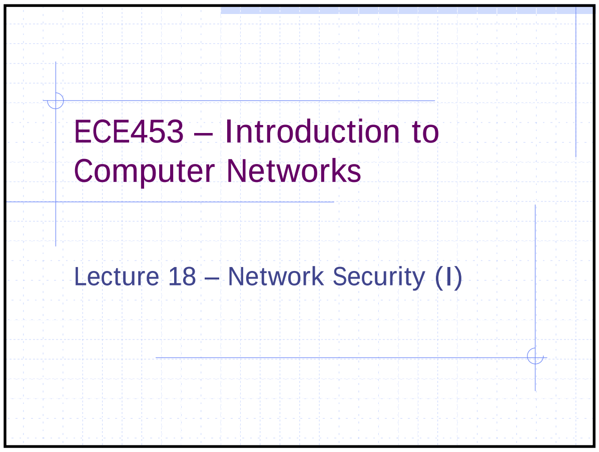
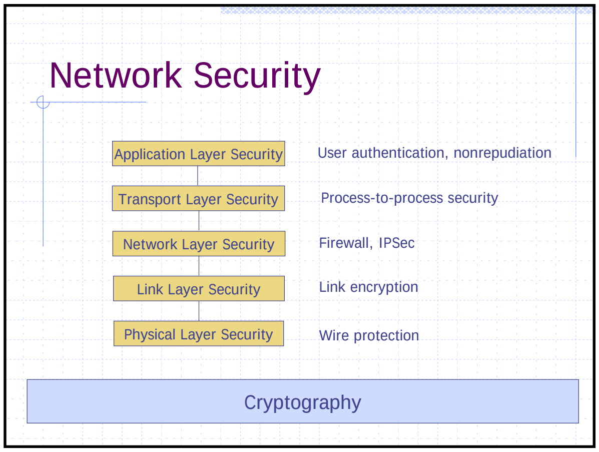


ECE453 – Introduction to Computer Networks

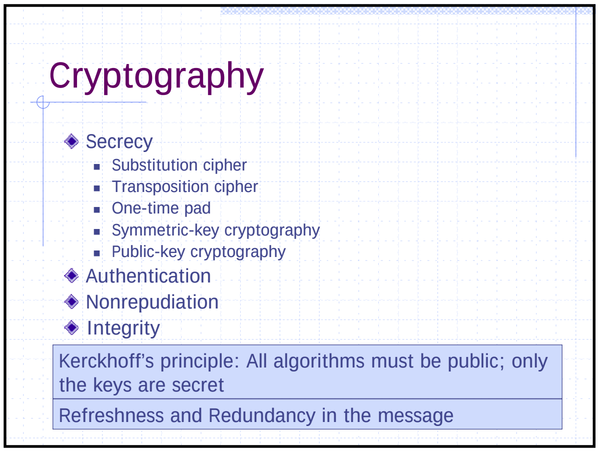
Lecture 18 – Network Security (I)



Network Security

Application Layer Security	User authentication, nonrepudiation
Transport Layer Security	Process-to-process security
Network Layer Security	Firewall, IPSec
Link Layer Security	Link encryption
Physical Layer Security	Wire protection

Cryptography

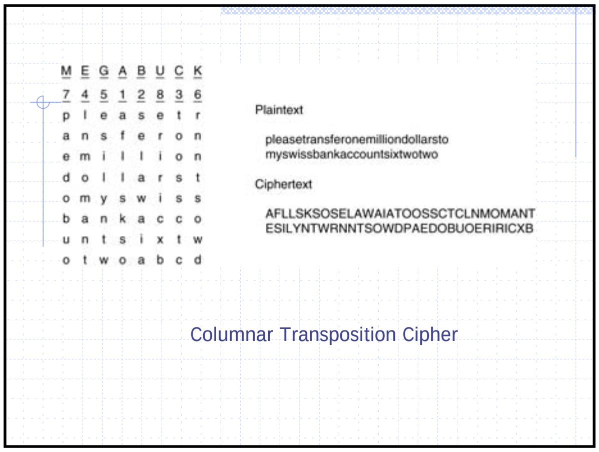


Cryptography

- Secrecy
  - Substitution cipher
  - Transposition cipher
  - One-time pad
  - Symmetric-key cryptography
  - Public-key cryptography
- Authentication
- Nonrepudiation
- Integrity

Kerckhoff's principle: All algorithms must be public; only the keys are secret

Refreshness and Redundancy in the message



M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

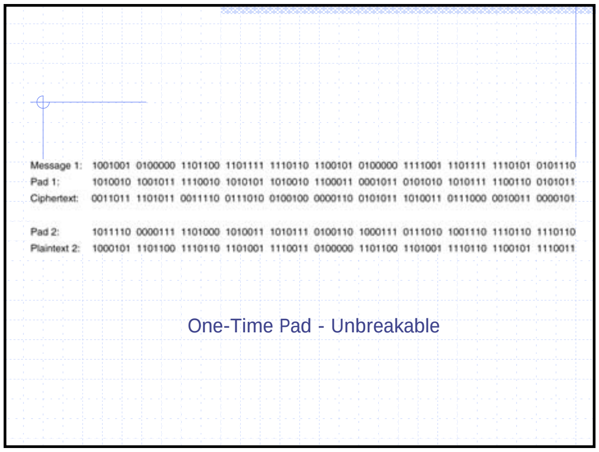
Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

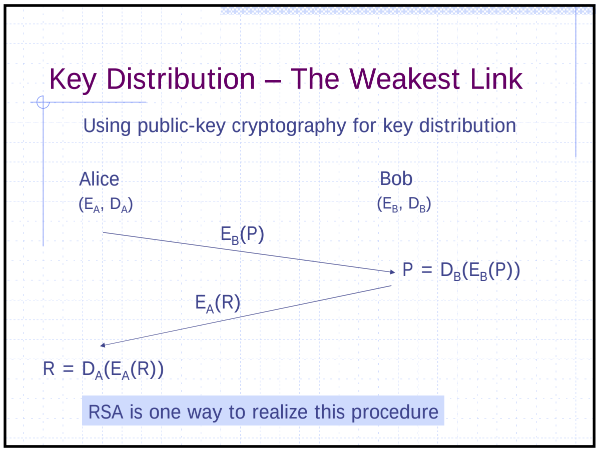
Columnar Transposition Cipher



```
Message 1:   1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
Pad 1:       1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
Ciphertext:  0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101

Pad 2:       1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
Plaintext 2: 1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011
```

One-Time Pad - Unbreakable



Key Distribution – The Weakest Link

Using public-key cryptography for key distribution

Alice

(E_A, D_A)

Bob

(E_B, D_B)

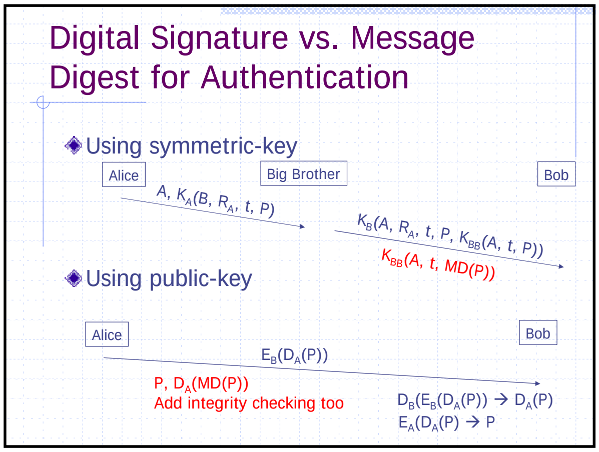
$E_B(P)$

$P = D_B(E_B(P))$

$E_A(R)$

$R = D_A(E_A(R))$

RSA is one way to realize this procedure



Digital Signature vs. Message Digest for Authentication

- Using symmetric-key

Alice

Big Brother

Bob

$A, K_A(B, R_A, t, P)$

$K_B(A, R_A, t, P, K_{BB}(A, t, P))$

$K_{BB}(A, t, MD(P))$

- Using public-key

Alice

Bob

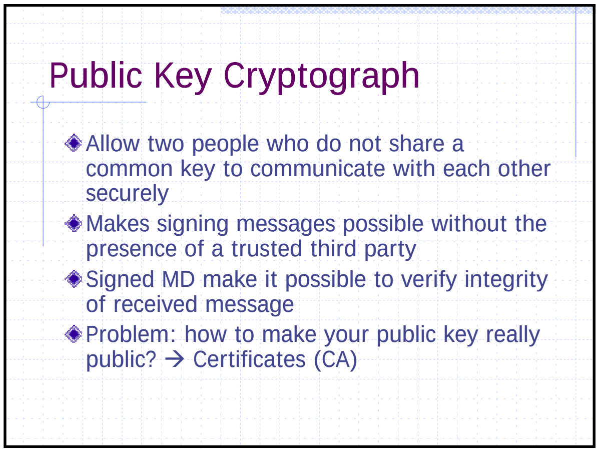
$E_B(D_A(P))$

P, $D_A(MD(P))$

Add integrity checking too

$D_B(E_B(D_A(P))$ → $D_A(P)$

$E_A(D_A(P)$ → P



Public Key Cryptograph

- Allow two people who do not share a common key to communicate with each other securely
- Makes signing messages possible without the presence of a trusted third party
- Signed MD make it possible to verify integrity of received message
- Problem: how to make your public key really public? → Certificates (CA)