

Information & Communication Security (SS 15)

Cryptography I

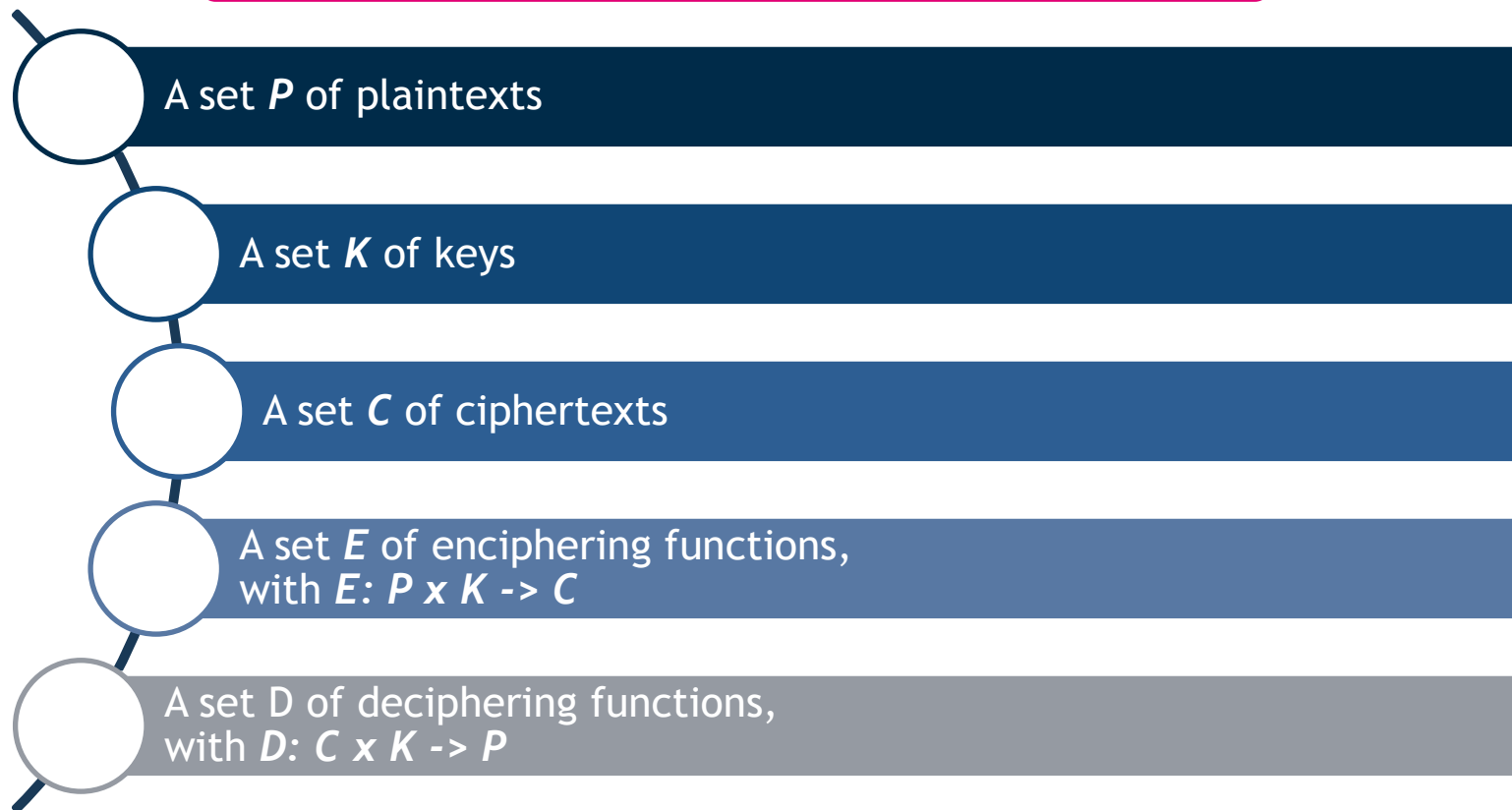
Dr. Jetzabel Serna-Olvera
@sernaolverajm

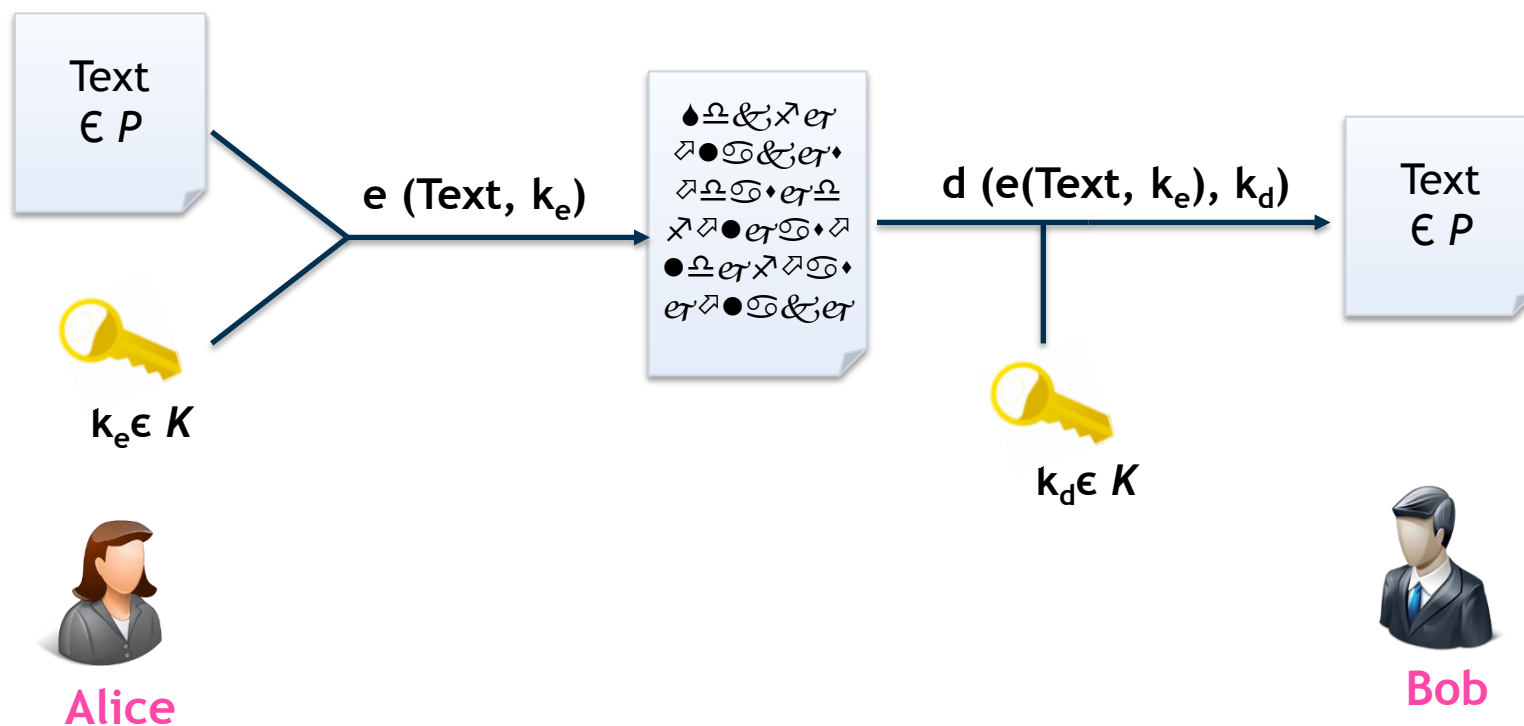
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

- Introduction
- Classical cryptosystems
 - General concept
 - Substitution ciphers
 - Caesar cipher
 - Vigenère cipher
 - One time pad
 - AES
 - Advantages and Problems
- Public key cryptography

Ciphertext
Public
Enigma
Asymmetric
AES
functions
Code
Hash
RSA
Symmetric
Key
Plaintext
Substitution
writing
Cipher
Secret

A Cryptosystem is a 5-tuple (P, K, C, E, D)



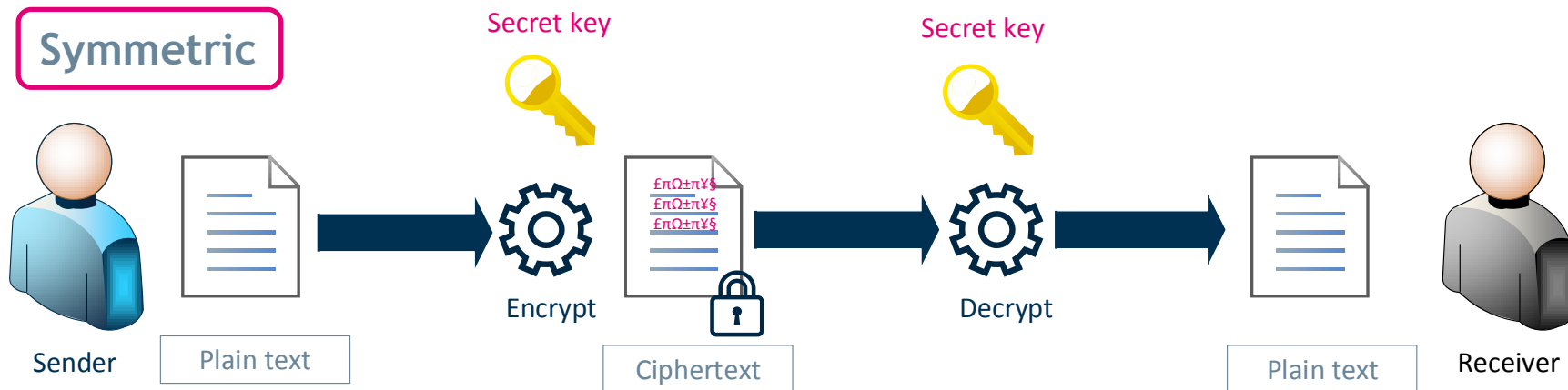


- Intention
 - Confidentiality (secrecy of messages):
encryption systems
 - Integrity (protection from undetected manipulation) and accountability:
authentication systems and **digital signature systems**
- Key distribution
 - Symmetric:
Both partners have the same key.
 - Asymmetric:
Different (but related) keys for encryption and decryption

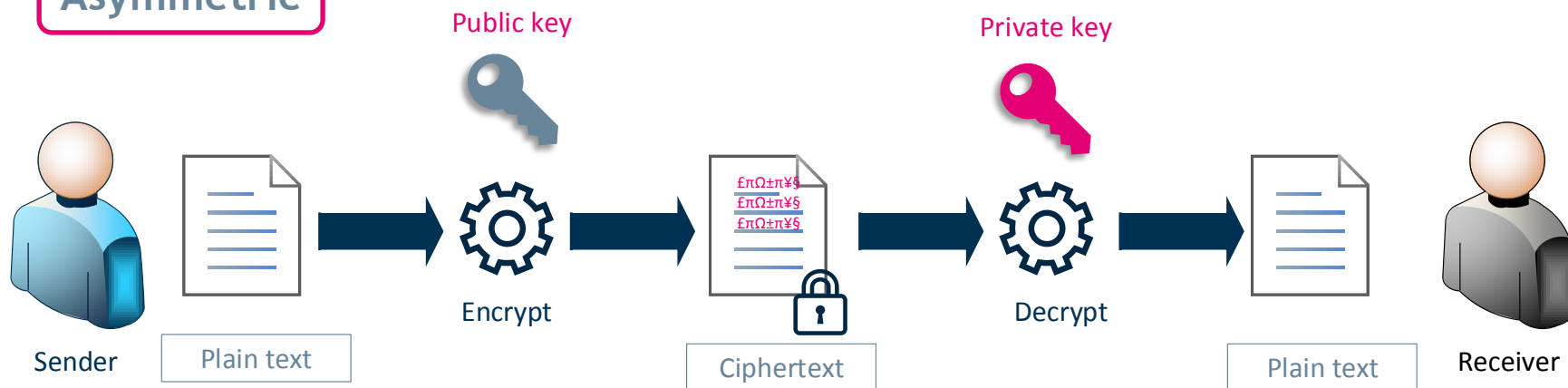
In practice mostly hybrid systems

Cryptographic Systems (II)

Symmetric

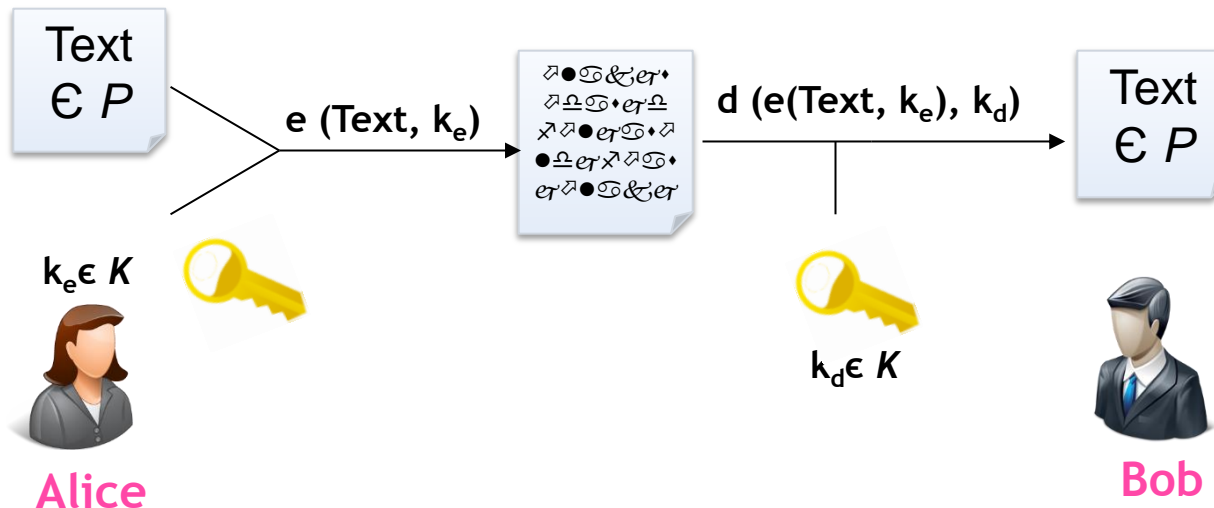


Asymmetric



Kerckhoffs' principle

- The principle (first stated in 1883):
 - The secret lies within the key and not within the algorithm;
 - Thus "Security through obscurity" is not a sustainable solution.
- In our small example:
 - Separation of algorithm e and key k_e



- In a ***ciphertext only*** attack, the adversary has only the ciphertext. Her goal is to find the corresponding plaintext. If possible, she may try to find the key, too.
- In a ***known plaintext*** attack, the adversary has the plaintext and the ciphertext that was enciphered. Her goal is to find the key that was used.
- In a ***chosen plaintext*** attack, the adversary may ask that specific plaintexts be enciphered. She is given the corresponding ciphertexts. Her goal is to find the key that was used.

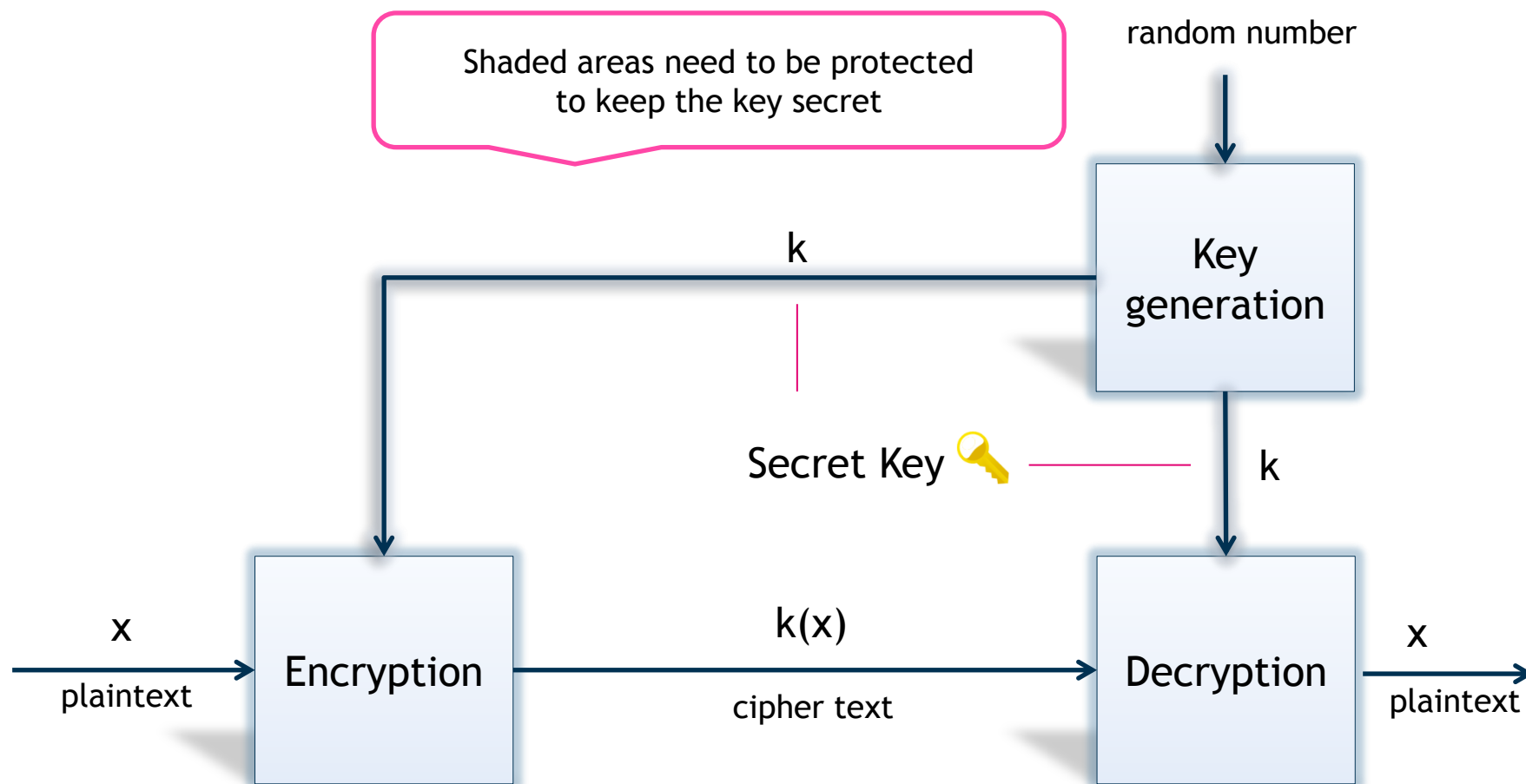
- Introduction
- Classical cryptosystems
 - General concept
 - Substitution ciphers
 - Caesar cipher
 - Vigenère cipher
 - One time pad
 - AES
 - Advantages and Problems
- Public key cryptography

Symmetric Encryption Systems

- Typical applications
 - confidential storage of user data
 - transfer of data between 2 users who negotiate a key via a secure channel
- Examples
 - Vernam-Code (one-time pad, Gilbert Vernam)
 - key length = length of the plaintext (information theoretically secure)
 - DES: Data Encryption Standard
 - key length 56 bit, so 2^{56} different keys
 - AES: Advanced Encryption Standard (Rijndael, [NIST])
 - 3 alternatives for key length: 128, 192 und 256 bit

- Introduction
- Classical cryptosystems
 - General concept
 - Substitution ciphers
 - Caesar cipher
 - Vigenère cipher
 - One time pad
 - AES
 - Advantages and Problems
- Public key cryptography

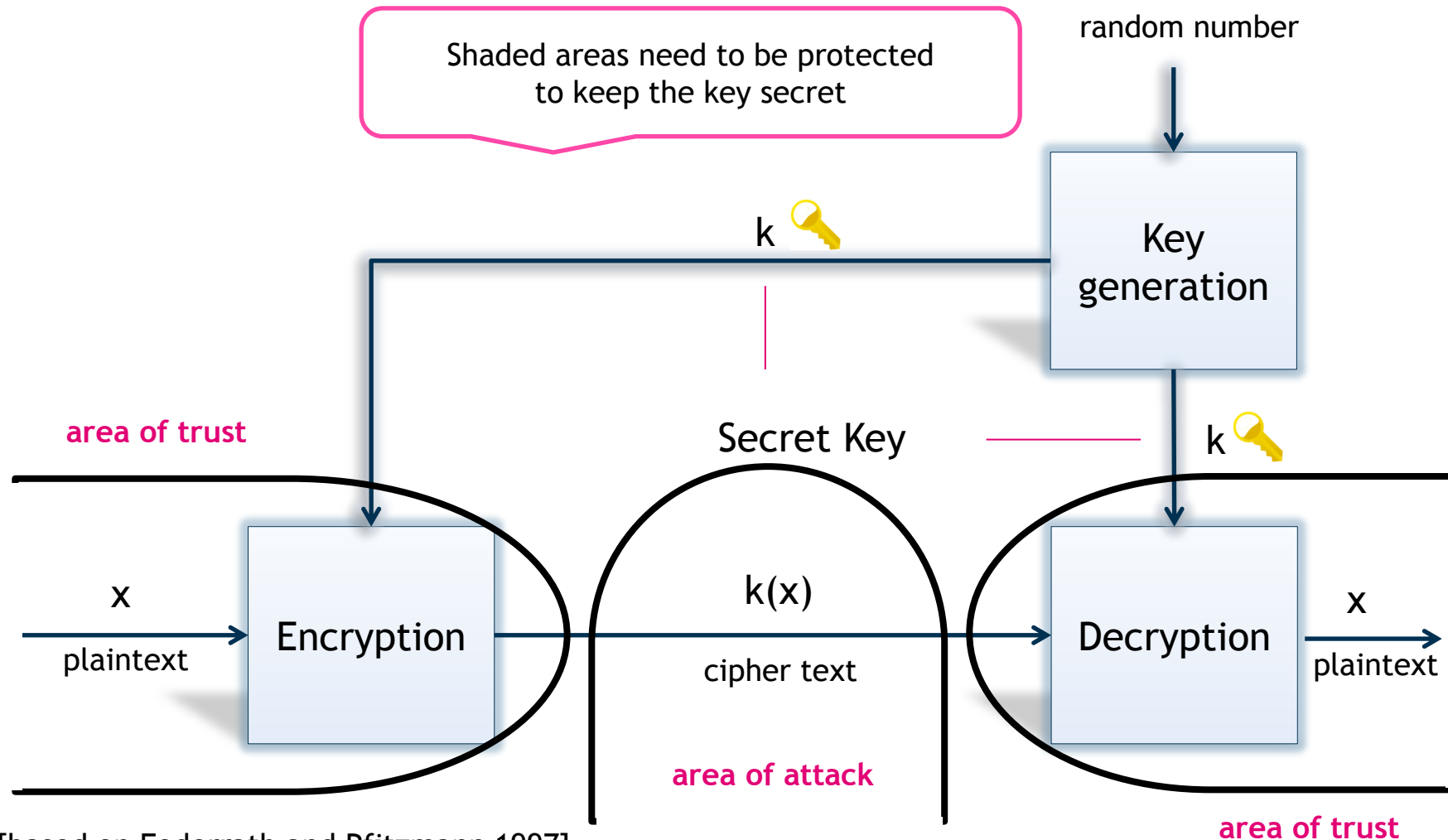
Symmetric Encryption Systems



[based on Federrath and Pfitzmann 1997]

Symmetric Encryption Systems

Shaded areas need to be protected
to keep the key secret



[based on Federrath and Pfitzmann 1997]

Symmetric Encryption Systems

- Keys have to be kept secret (*secret key crypto system*).
- It must not be possible to infer on the plaintext or the keys used from the encrypted text (ideally encrypted text is not distinguishable from a numerical random sequence).
- Each key shall be equally probable.
- In principle each system with limited key length is breakable by testing all possible keys.
- *Publication of encrypting and decrypting functions (algorithms) is considered as good style and is trust-building.*
- Security of cryptosystems should base on the strength of chosen key lengths.

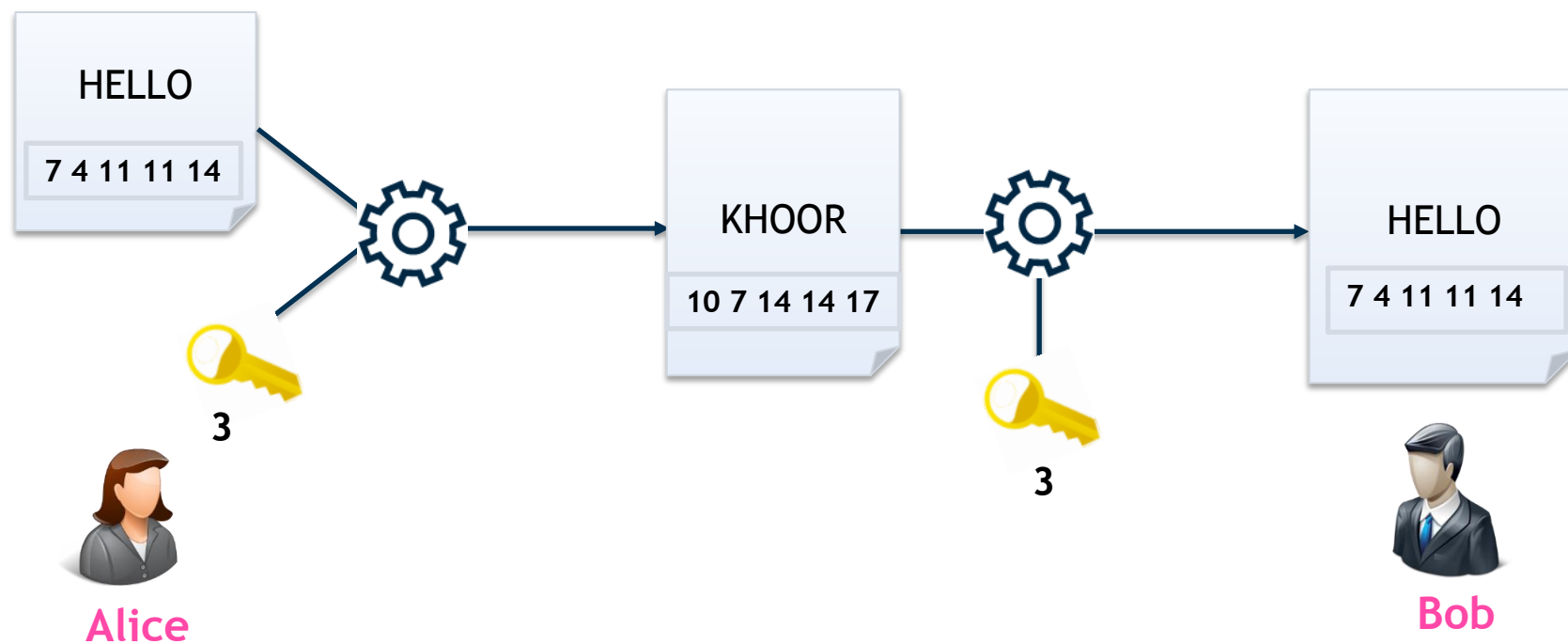
- Introduction
- Classical cryptosystems
 - General concept
 - Substitution ciphers
 - Caesar cipher
 - Vigenère cipher
 - One time pad
 - AES
 - Advantages and Problems
- Public key cryptography

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- We assign a **number** for **every** character.
- This enables us to calculate with letters as if they were numbers.

- For $k \in \{0..25\}$ we have:
 - An encryption function:
 - $e: x \rightarrow (x+k) \bmod 26$
 - A decryption function:
 - $d: x \rightarrow (x-k) \bmod 26$
 - In this case $k_e = k_d$



- In case of a known plaintext attack it is trivial to get the key used.
- There are only 26 possible keys. This cipher is therefore vulnerable to a **brute force attack**.
- This cipher is also vulnerable to a **statistical ciphertext-only attack**.

Assessment of Caesar Cipher

- Of course this is a very simple form of encryption.
- The encryption and decryption algorithms are very easy and fast to compute.
- It uses a very limited key space ($n=26$).
- Therefore, the encryption is very easy and fast to compromise.

Can We Make it More Secure?

- Use a permutation of the alphabet as the key.
- Example:

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

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

- “HELLO” -> “ITSSG”

- Use of permutations increases the key space.
- Therefore, a **brute force attack** becomes more difficult.
- The encryption and decryption are not much harder to compute.
 - Table lookup
- Still vulnerable to a **statistical ciphertext-only attack**.

Statistical Ciphertext-only Attack

- Use statistical frequency of occurrence of single characters to figure out the key.
- Language dependent
- Frequencies of character pairs (bigrams) may also be used

E	11.1607%	M	3.0129%
A	8.4966%	H	3.0034%
R	7.5809%	G	2.4705%
I	7.5448%	B	2.0720%
O	7.1635%	F	1.8121%
T	6.9509%	Y	1.7779%
N	6.6544%	W	1.2899%
S	5.7351%	K	1.1016%
L	5.4893%	V	1.0074%
C	4.5388%	X	0.2902%
U	3.6308%	Z	0.2722%
D	3.3844%	J	0.1965%
P	3.1671%	Q	0.1962%

(English)

[<http://www.oxforddictionaries.com/words/what-is-the-frequency-of-the-letters-of-the-alphabet-in-english>]

- Introduction
- Classical cryptosystems
 - General concept
 - Substitution ciphers
 - Caesar cipher
 - Vigenère cipher
 - One time pad
 - AES
 - Advantages and Problems
- Public key cryptography

- The Vigenère cipher chooses a sequence of keys, represented by a string.
- The key letters are applied to successive plaintext characters.
- When the end of the key is reached, the key starts over.
- The length of the key is called the *period* of the cipher.

Vigenère Tableau

	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

Example

- Let the message be "THE BOY HAS THE BAG"
- and let the KEY be "VIG"

PT= T H E B O Y H A S T H E B A G

K= V I G V I G V I G V I G V I G

CT= O P K W W E C I Y O P K W I M

Assessment Vigenère Cipher

- For many years, the Vigenère cipher was considered unbreakable.
- Then a Prussian cavalry officer named Kasiski noticed that repetitions occur when characters of the key appear over the same characters in the plaintext.
- The number of characters between successive repetitions is a multiple of the period (key length).
- Given this information and a short period the Vigenère cipher is quite easily breakable.
- *Example: The Caesar cipher is a Vigenère cipher with a period of 1.*

Example Vigenère Cipher

- Let the message be „THE BOY HAS THE BAG “ and let the key be „VIG “:

- Plaintext: T H E B O Y H A S T H E B A G
- Key: V I G V I G V I G V I G V I G
- Ciphertext: O P K W W E C I Y O P K W I M

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


Example

- Let the message be "HELLO"
- and let the KEY be "SEC"
- a=ZINLO
- b=ZINDS
- c=ZENNO

- Introduction
- Classical cryptosystems
 - General concept
 - Substitution ciphers
 - Caesar cipher
 - Vigenère cipher
 - One time pad
 - AES
 - Advantages and Problems
- Public key cryptography

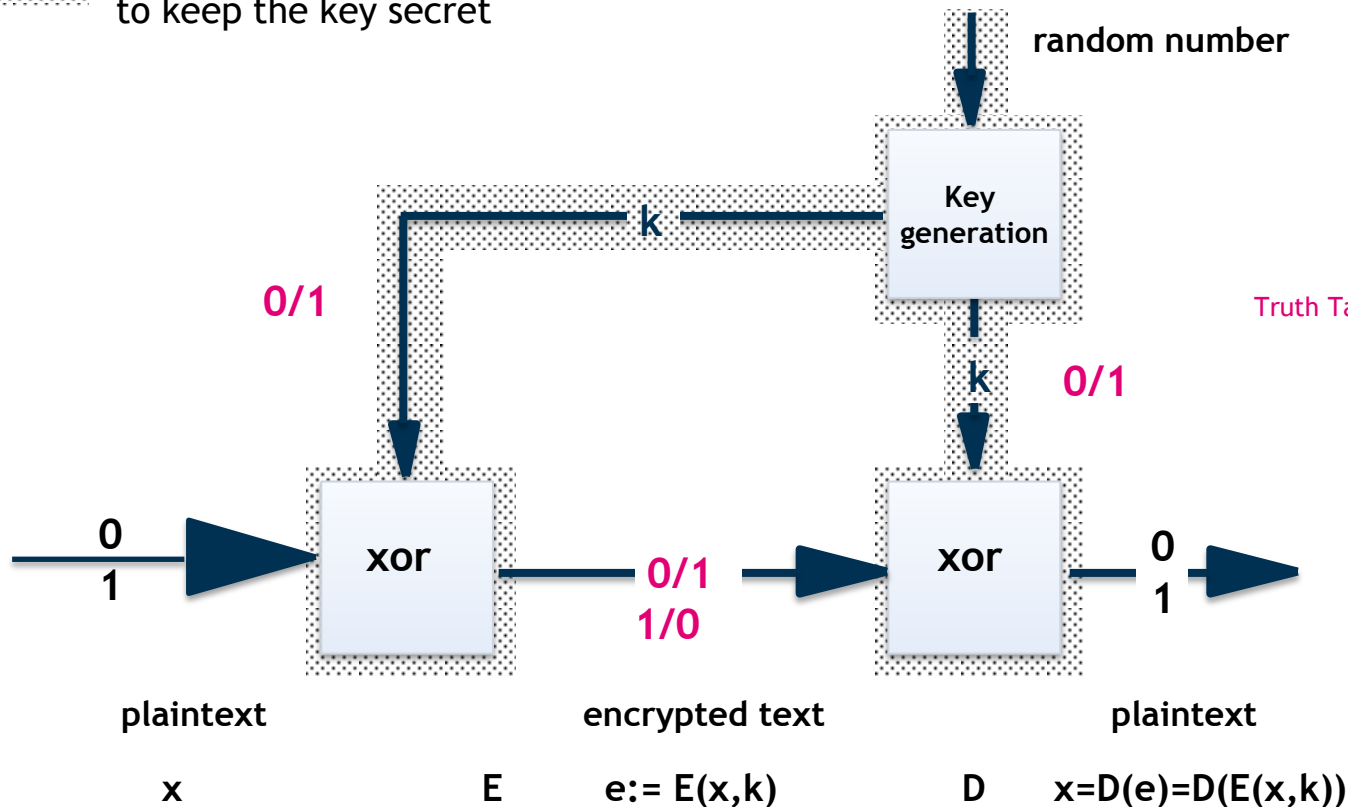
- Invented by Gilbert Vernam
- The one-time pad is basically a Vigenère cipher.
- The length of the key is as long as the length of the plaintext.
- Therefore, there are no periodic reoccurrences.
- The key is randomly chosen and only used once.
- Every key has the same probability.

Example One Time Pad

 area that needs to be protected to keep the key secret

X_i	S_i	Y_i
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table of the XOR operation



[based on Federrath and Pfitzmann 1997]

Example

PT=	0	1	1	0
k=	1	0	1	1

X_i	S_i	Y_i
0	0	0
0	1	1
1	0	1
1	1	0

Truth Table of the XOR operation

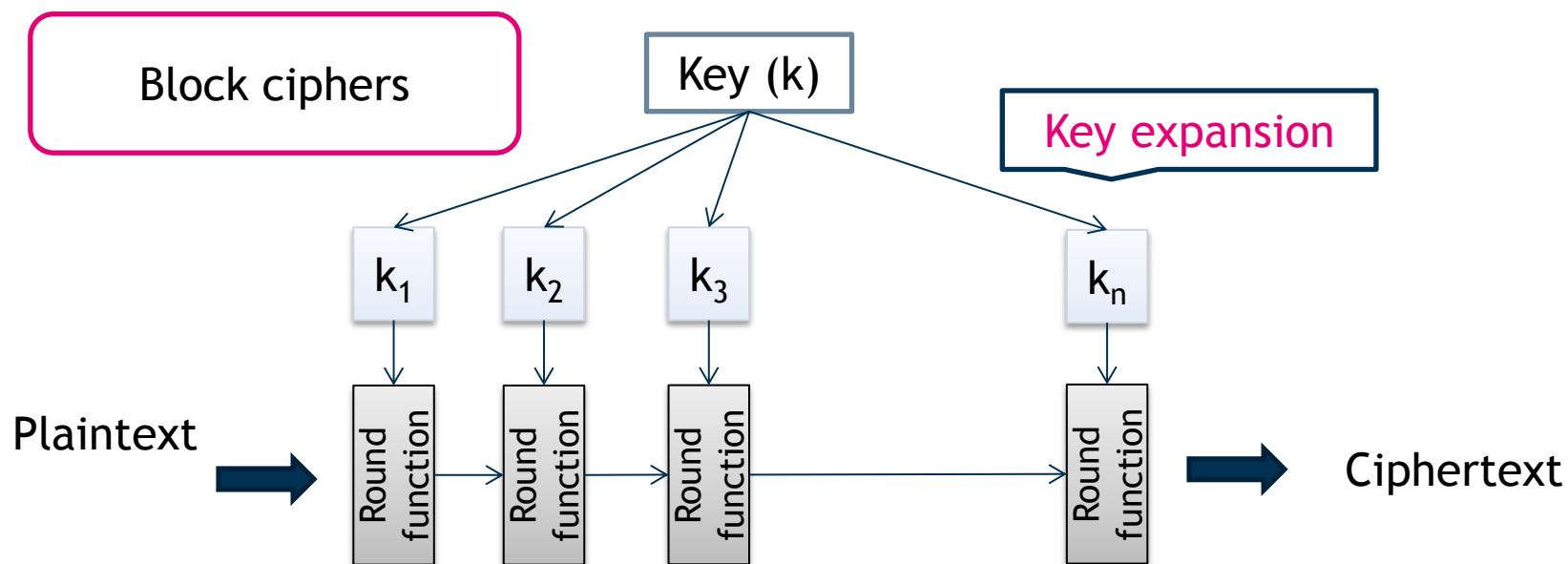
a=	1	1	1	1
b=	1	0	1	1
c=	1	1	0	1

Assessment One Time Pad

- The one time pad is unbreakable by ciphertext only attacks.
 - Example: Let the ciphertext be “FGHA” .
 - Since we know the key length is at least 4 and the probability of every possible key is equal, the plaintext can be any 4-letter word possible.
- In a known plaintext attack we can deduct the key.
 - Then we know which key was used to encrypt the message we already know.
 - But the next message is encrypted with a different key, because every key is only used once.
- The same applies to a chosen plaintext attack.
- **The one-time pad is information theoretically secure and provably impossible to break.**

- Introduction
- Classical cryptosystems
 - General concept
 - Substitution ciphers
 - Caesar cipher
 - Vigenère cipher
 - One time pad
 - AES
 - Advantages and Problems
- Public key cryptography

Advanced Encryption Standard



- This new cipher is called Advanced Encryption Standard (AES).
- AES has been approved for Secret or even Top Secret information by the NSA.

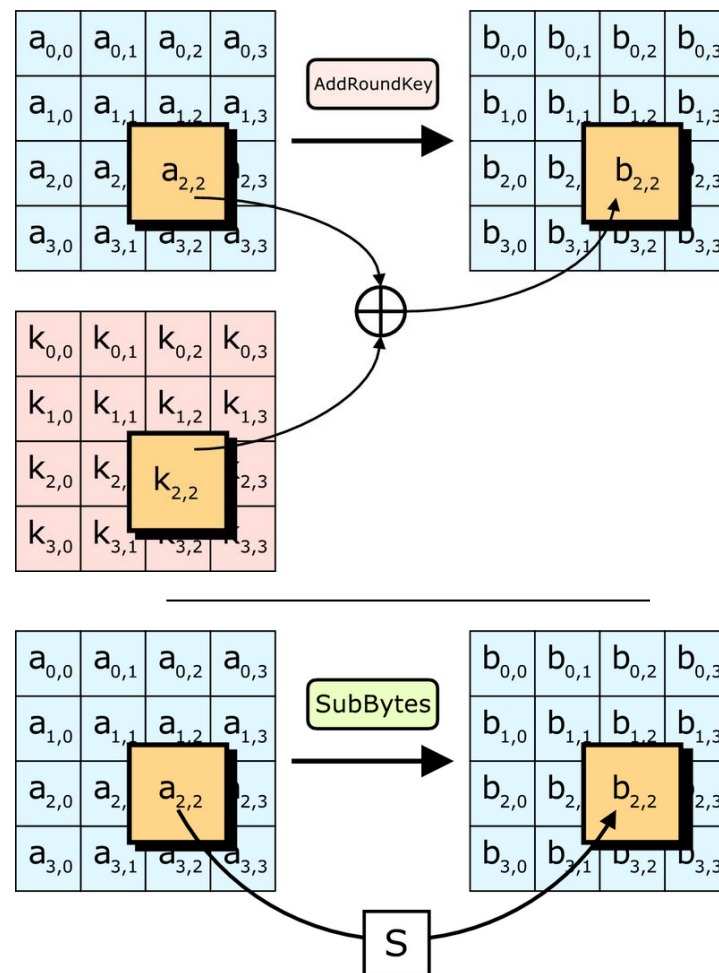
AES Encryption - Overview

- AES encryption
 - has a variable **number of rounds (10, 12, 14)**
 - depending on **key size (128-bit, 192-bit, 256-bit)**.
- To encipher a block of data in AES
 - Initialize (key schedule...)
 - Stretch key data
 - Initialization Round
 - Then several rounds of encryption
 - Shifting and mixing bits
 - Finally, some postprocessing
 - perform a round with the last step omitted

Encryption Round (1)

AES

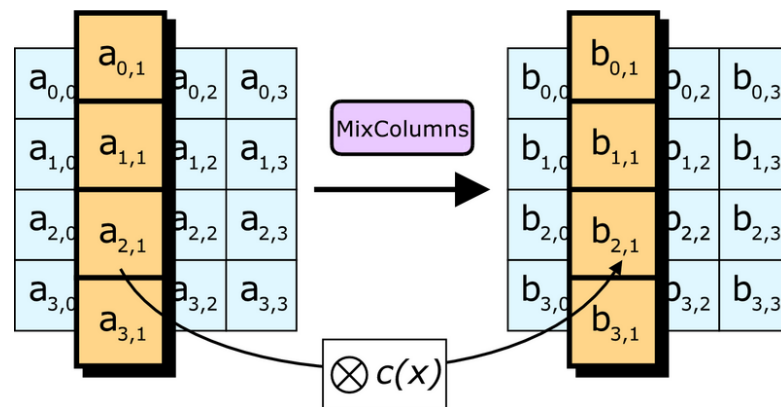
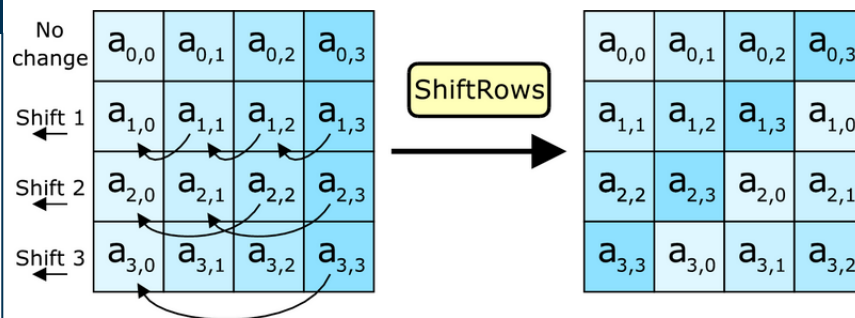
- AddRoundKey
 - XOR (mix bits of) current state a and round key
 - Round key k derived using key schedule
- SubBytes
 - Substitution using a lookup table (S-Box)



Encryption Round (2)

AES

- **ShiftRows**
 - Shift each row by row index
- **MixColumns**
 - 4 key bytes combined into each column using polynomial multiplication modulo 2^8 [in $GF(2^8)$]



- Introduction
- Classical cryptosystems
 - General concept
 - Substitution ciphers
 - Caesar cipher
 - Vigenère cipher
 - One time pad
 - AES
 - Advantages and Problems
- Public key cryptography

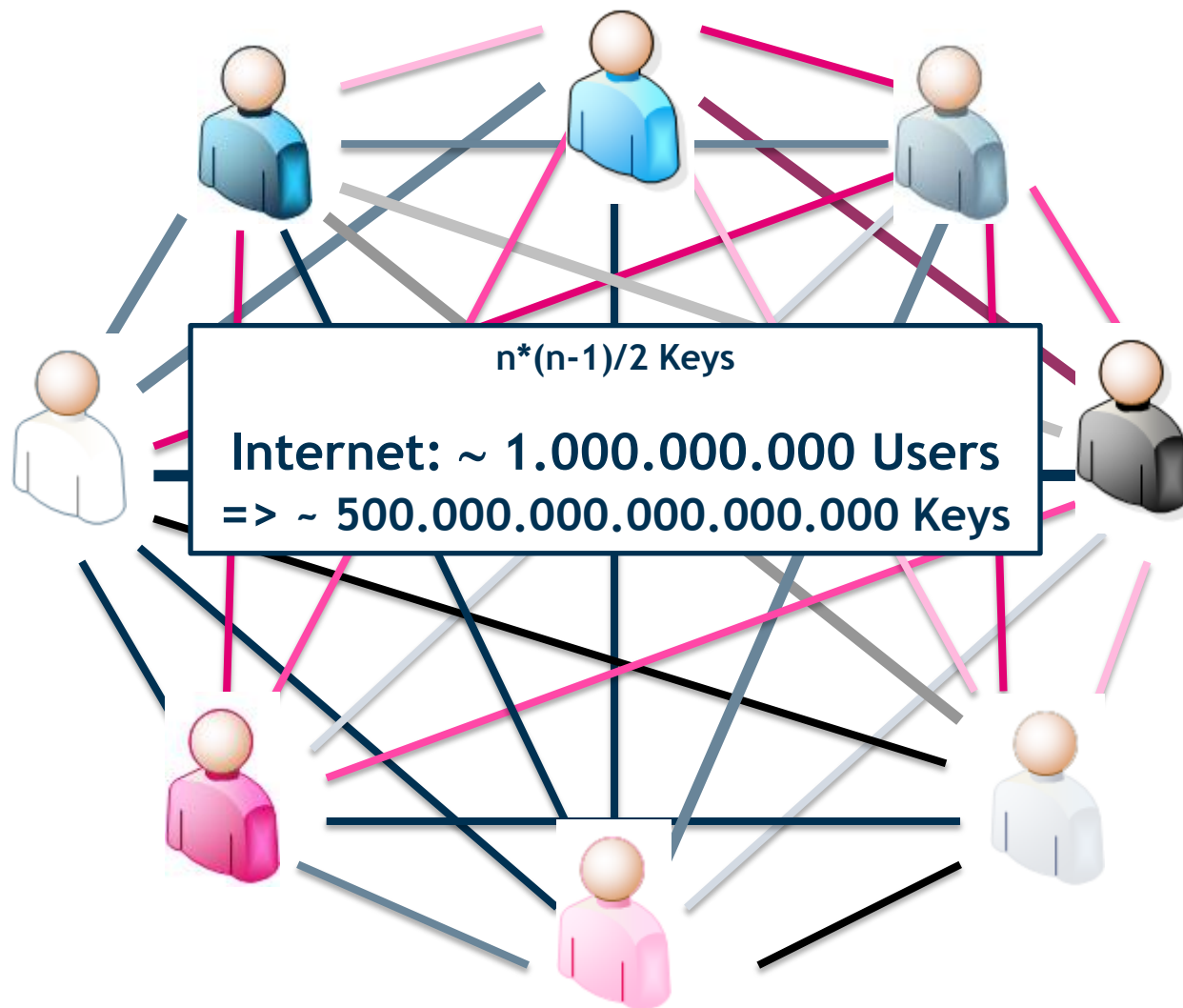
Symmetric Encryption

Advantage: Algorithms are very fast

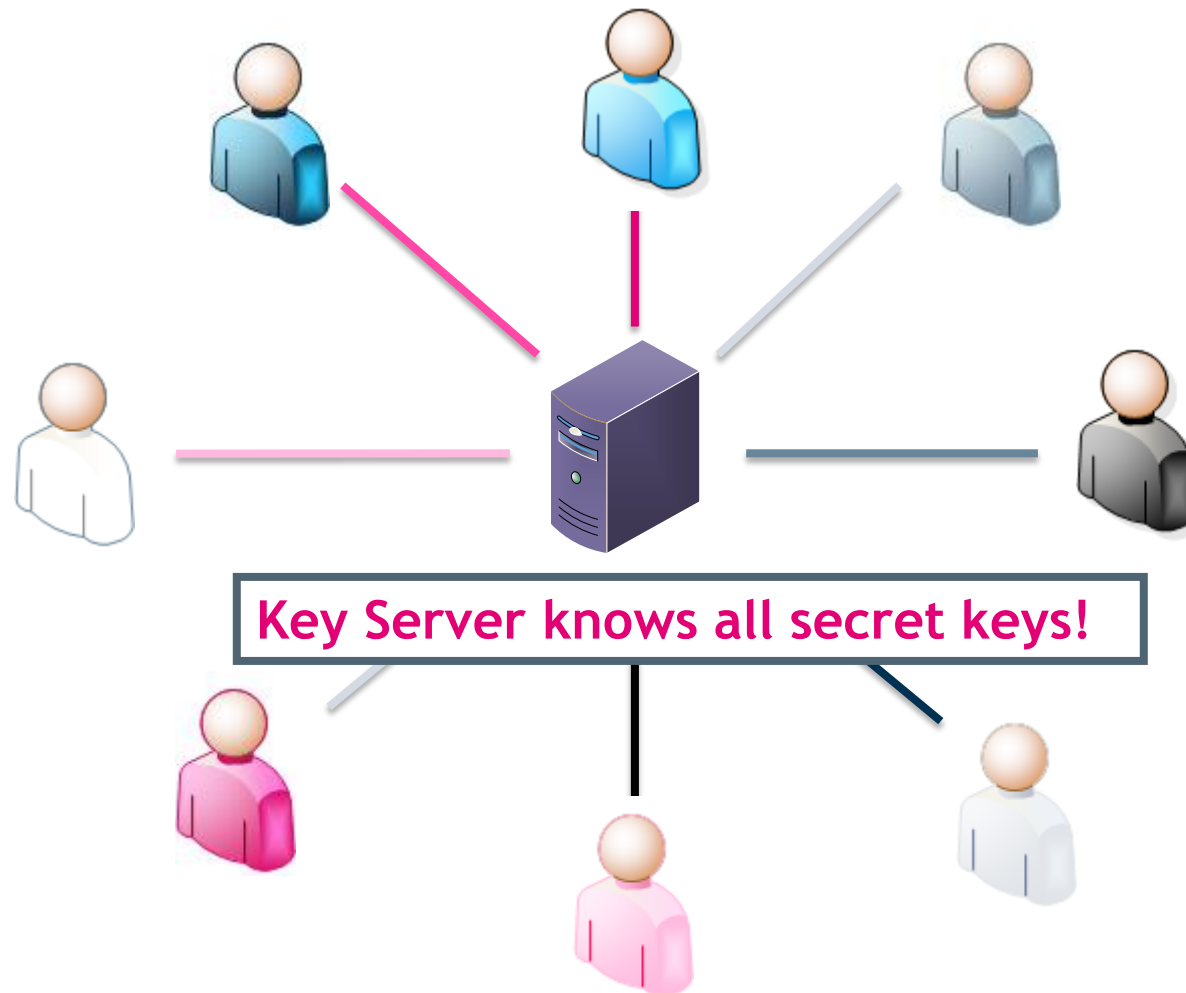
Algorithm	Performance [*]
RC6	78 ms
SERPENT	95 ms
IDEA	170 ms
MARS	80 ms
TWOFISH	100 ms
DES-edc	250 ms
RIJNDEAL (AES)	65 ms

*** Encryption of 1 MB on a Pentium 2.8 GHz, using the FlexiProvider Java)**

Disadvantage: Key Exchange

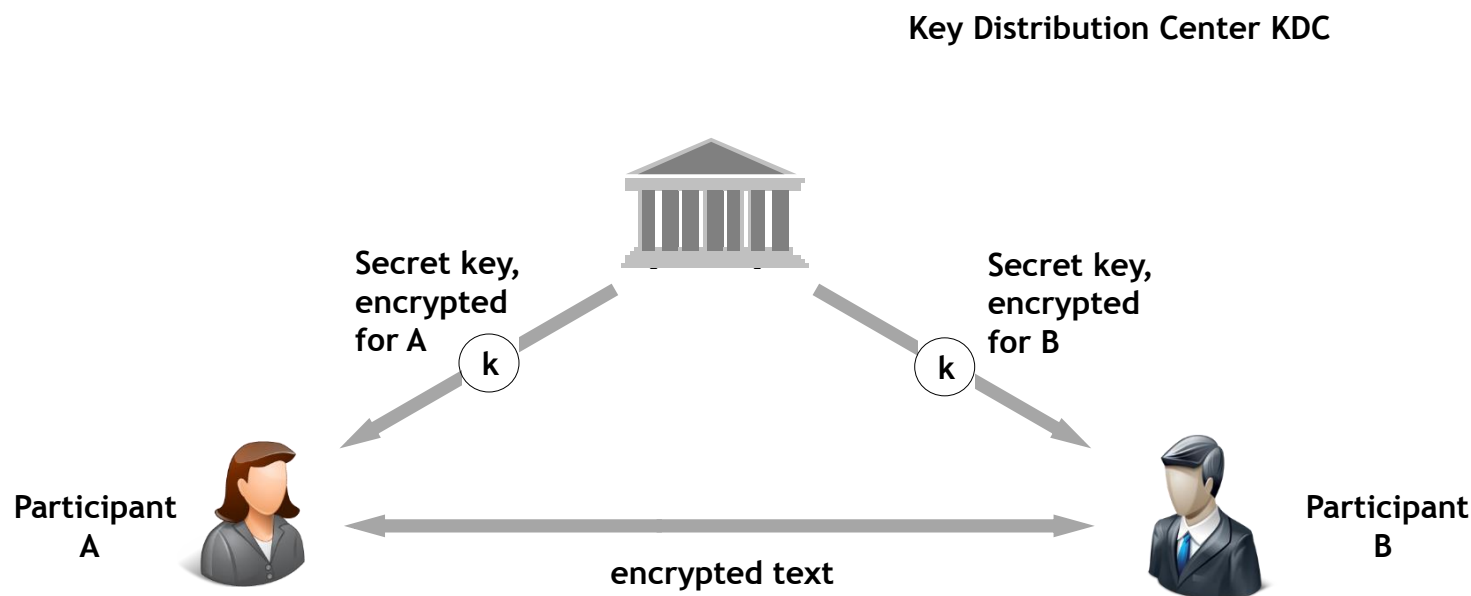


A Possible Solution



Key Management in Symmetric Encoding Systems

- One key per communication pair is necessary.
- Secure agreement and transfer are also challenging.
- A center for key distribution is possible but this party then knows all secret keys!



Roger Needham / Butler Lampson

“Anybody who asserts that a problem is readily solved by encryption, understands neither encryption nor the problem.”



[Marshall Symposium 1998] [Randell 2004]

- **[Bi2005] Matt Bishop:** *Introduction to Computer Security*. Boston: Addison Wesley, 2005. pp. 97-113
- **[The Marshall Symposium] The Marshall Symposium:** Address Roger Needham, May 29, 1998, Rackham School of Graduate Studies, University of Michigan
web.archive.org/web/20081201182254/http://www.si.umich.edu/marshall/docs/p201.htm, accessed 2015-04-15.
- **[Randell 2004] Randell, B. (2004) *Brief Encounters*;** Pp. 229-235 in: Andrew Herbert, Karen Spärck Jones: *Computer Systems: Theory, Technology, and Applications*; New York, Springer 2004
- **[Federrath Pfitzmann 1997] Hannes Federrath, Andreas Pfitzmann:** Bausteine zur Realisierung mehrseitiger Sicherheit. in: Günter Müller, Andreas Pfitzmann (Hrsg.): *Mehrseitige Sicherheit in der Kommunikationstechnik*, Addison-Wesley-Longman 1997, 83-104.



Deutsche Telekom Chair of Mobile Business & Multilateral Security

Dr. Jetzabel M. Serna-Olvera

Goethe University Frankfurt

E-Mail: Jetzabel.Serna-Olvera@m-chair.de

WWW: www.m-chair.de