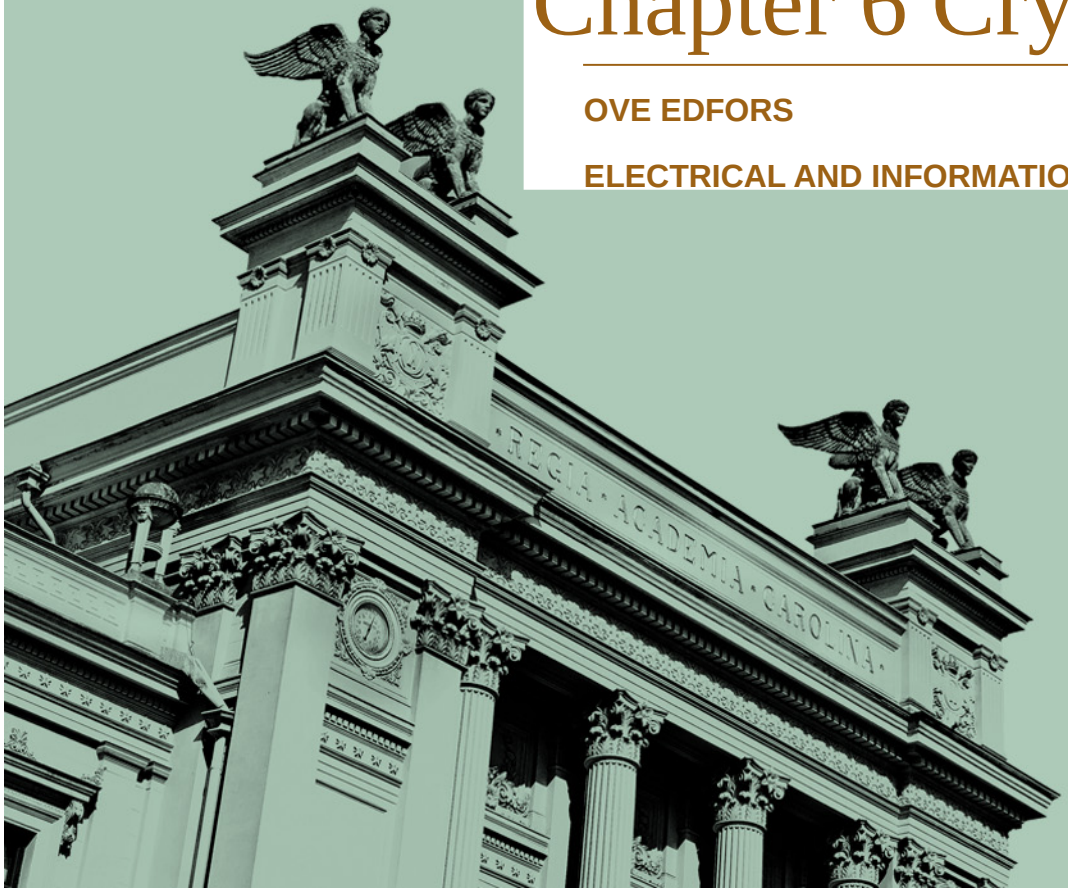
LUND UNIVERSITY

Information Transmission
Chapter 6 Cryptology

OVE EDFORS

ELECTRICAL AND INFORMATION TECHNOLOGY



Learning outcomes

- After this lecture the student should
  - undertand what cryptology is and how it is used,
  - be familiar with the crypto models of systems for secrecy and authentication,
  - understand what makes a crypto system secure,
  - be able to perform encryption, decryption and cryptanalysis on simple ciphers,
  - understand how Cesar, Viginere and Vernam ciphers work, and
  - understand the principle of perfect security.

LUND UNIVERSITY

Cryptology

"The science concerned with data communication and storage in secure and usually secret form" – Encyclopaedia Britannica

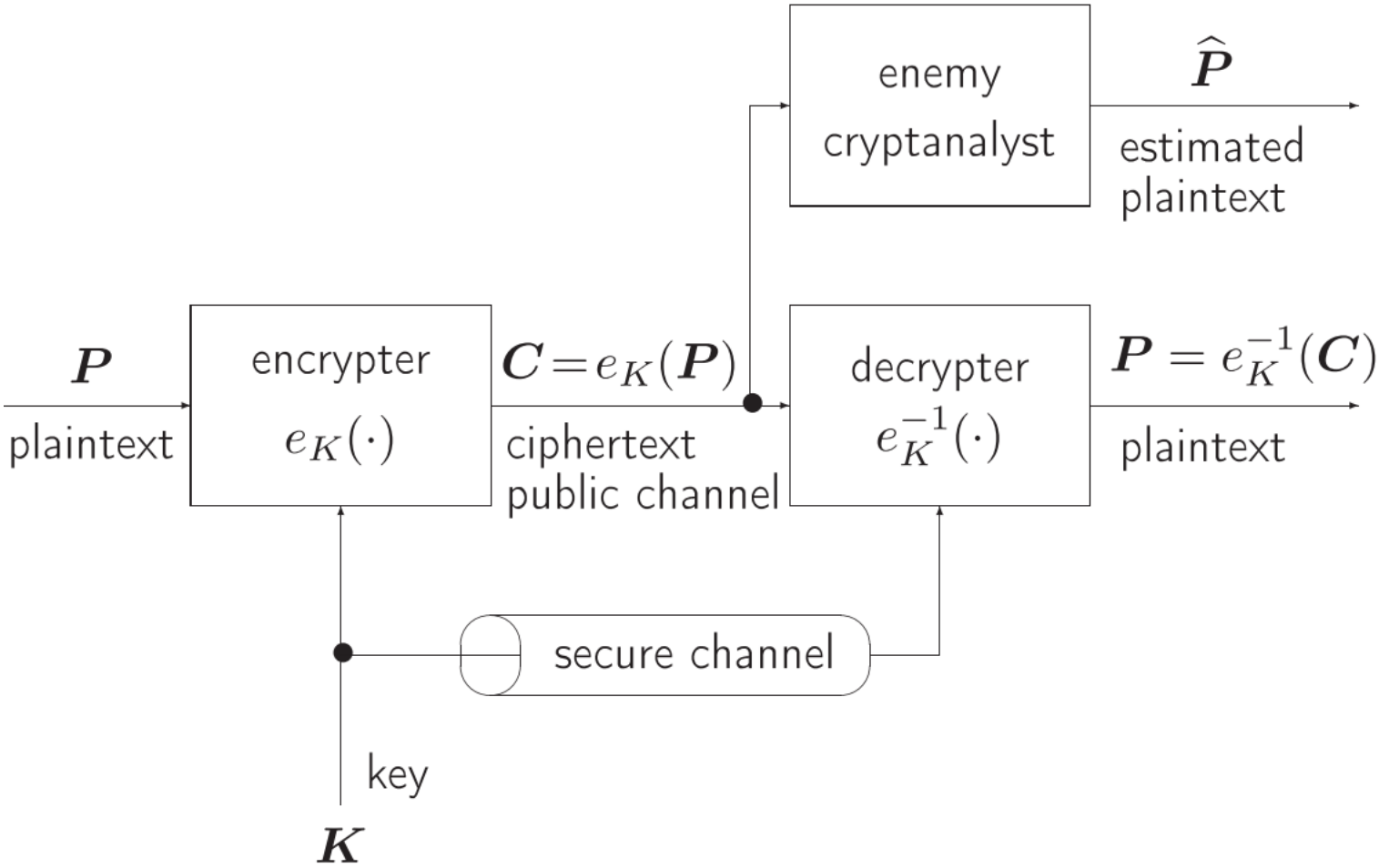
Legitimate users obtain security by using a secret key that is known only to them.

The area is often subdivided into the two disciplines:

- Cryptography
- Cryptanalysis

LUND UNIVERSITY

Model of a cryptosystem for secrecy

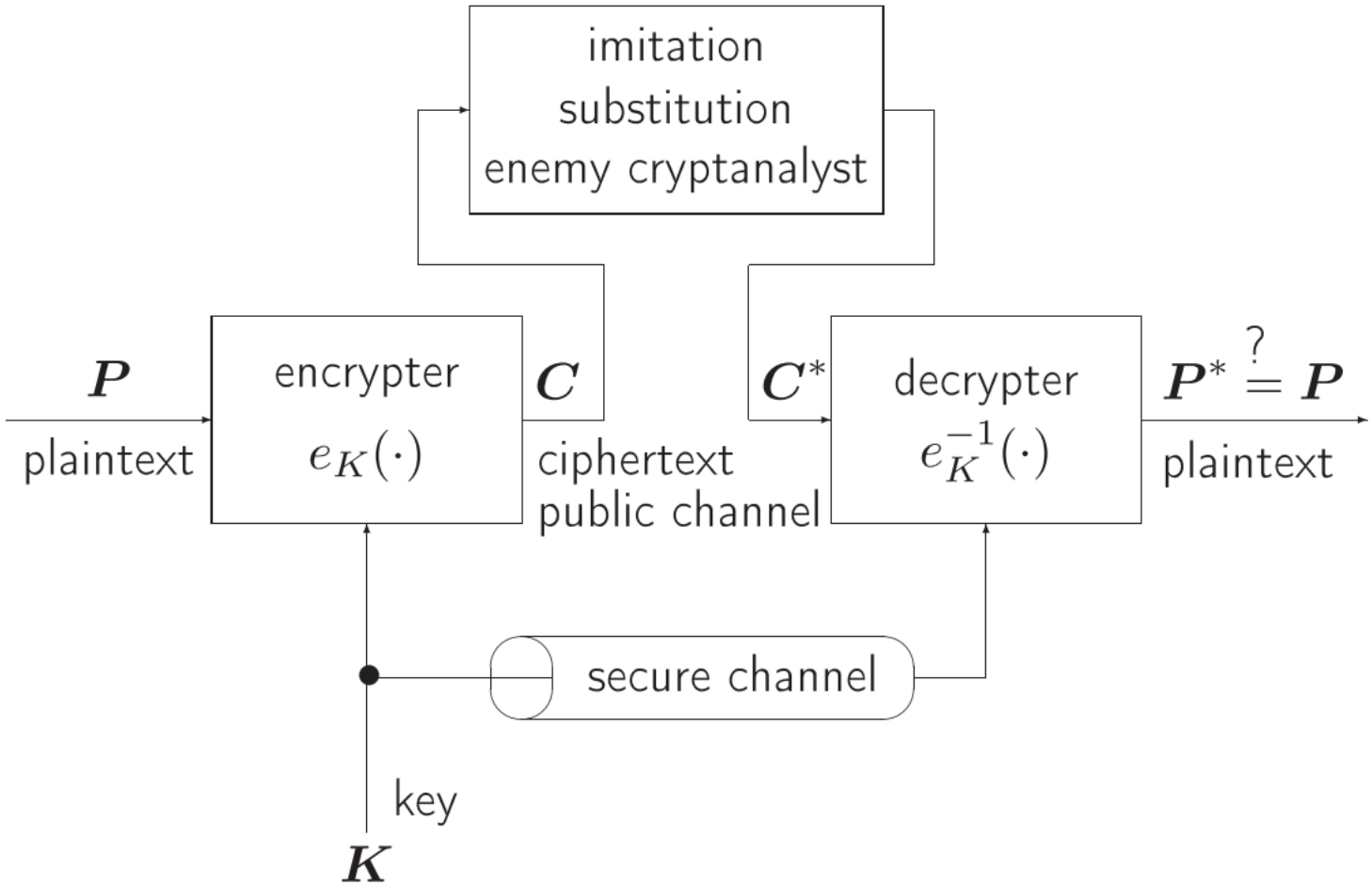


Security of the cipher

- The security of the cipher should reside entirely in the secret key.
- The designer of a cryptosystem should always assume that the enemy ``by hook or by crook'' can get hold of a detailed description of the cryptosystem; the only thing that is hidden from the cryptanalyst is the actual value of the key.
- Although this is an old principle formulated by Auguste Kerckhoffs already in 1883, it is still valid

LUND UNIVERSITY

Model of a cryptosystem for authentication



Impersonation and substitution

The impersonation attack is successful if the receiver accepts the ciphertext **C*** that is chosen by the intruder *without knowledge about the genuine ciphertext* **C**

In the substitution attack the intruder first observes the genuine ciphertext **C**, then he chooses a ciphertext **C*** that he hopes will be accepted by the receiver.

LUND UNIVERSITY

Probability of a successful impersonation attack

Simmons showed a combinatorial lower bound on the probability of a successful impersonation attack, namely,

$$Pr(I) \geq \frac{|\mathcal{P}|}{|\mathcal{C}|}$$

where $|\mathcal{P}|$ and $|\mathcal{C}|$ are the numbers of plaintexts and ciphertexts, respectively.

Caesar and Vigenère ciphers

Caesar shifted the cipher alphabet three steps such that

A is encrypted as D

B is encrypted as E

C is encrypted as F

As an example we have

plaintext	ciphertext
CAESAR	FDHVDU

Caesar used always a shift of three steps, but nowadays a cipher obtained by any shift is called a *Caesar cipher*. The number of steps in the shift is the key; that is, the classical Caesar cipher has key K=3.

LUND UNIVERSITY

```
DIAJMHVODJI
EJBKNIWPEKJ
FKCLOJXQFLK
GLDMPKYRGML
HMENQLZSHNM
INFORMATION
JOGPSNBUJPO
KPHQTOCVKQP
LQIRUPDWLRQ
MRJSVQEXMSR
NSKTWRFYNTS
OTLUXSGZOUT
PUMVYTHAPVU
QVNWZUIBQWV
RWOXAVJCRXW
SXPYBWKDSYX
TYQZCXLETZY
UZRADYMFUAZ
VASBEZNGVBA
WBTCFAOHWCB
XCUDGBPIXDC
YDVEHCQJYED
ZEWFIDRKZFE
AFXGJESLAGF
BGYHKFTMBHG
CHZILGUNCIH
```

Cryptanalysis of a Caesar cipher.

Mono-alphabetic substitution ciphers

The Caesar cipher is a special case of a mono-alphabetic substitution cipher: An arbitrary permutation of the English alphabet is used as the key for a substitution done letter by letter.

For example, the mapping

Plaintext alphabet	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher alphabet	XGUACDTBFHRSLMQVYZWIEJOKNP

is a key that enciphers the plaintext WOODSTOCK as the ciphertext OQQAWIQUR.

LUND UNIVERSITY

The Vigenère cipher

To make a cipher less vulnerable to statistical attacks we can try to conceal the varying relative frequencies for the plaintext letters by using more than one substitution alphabet.

A popular example of a so called *polyalphabetic substitution cipher* is the *Vigenère cipher* named after the French cryptographer Blaisede Vigenère (1523--1596).

For a couple of centuries his cipher was known as *le chiffre indéchiffrable*, the ”unbreakable cipher".

LUND UNIVERSITY

	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

The Vigenère cipher

The key consists of a word that is repeated periodically. For example, if the key is THOMPSON and the plaintext is FOR WOODSTOCK MY FRIEND OF FRIENDS, then we obtain the ciphertext as follows:

plaintext	FORWOODSTOCKMYFRIENDOFFRIENDS
key	THOMPSONTHOMPSONTHOMPSONTHOMP
ciphertext	YVFIDGRFMVQWBQTEBLBPDXTEBLBPH

LUND UNIVERSITY

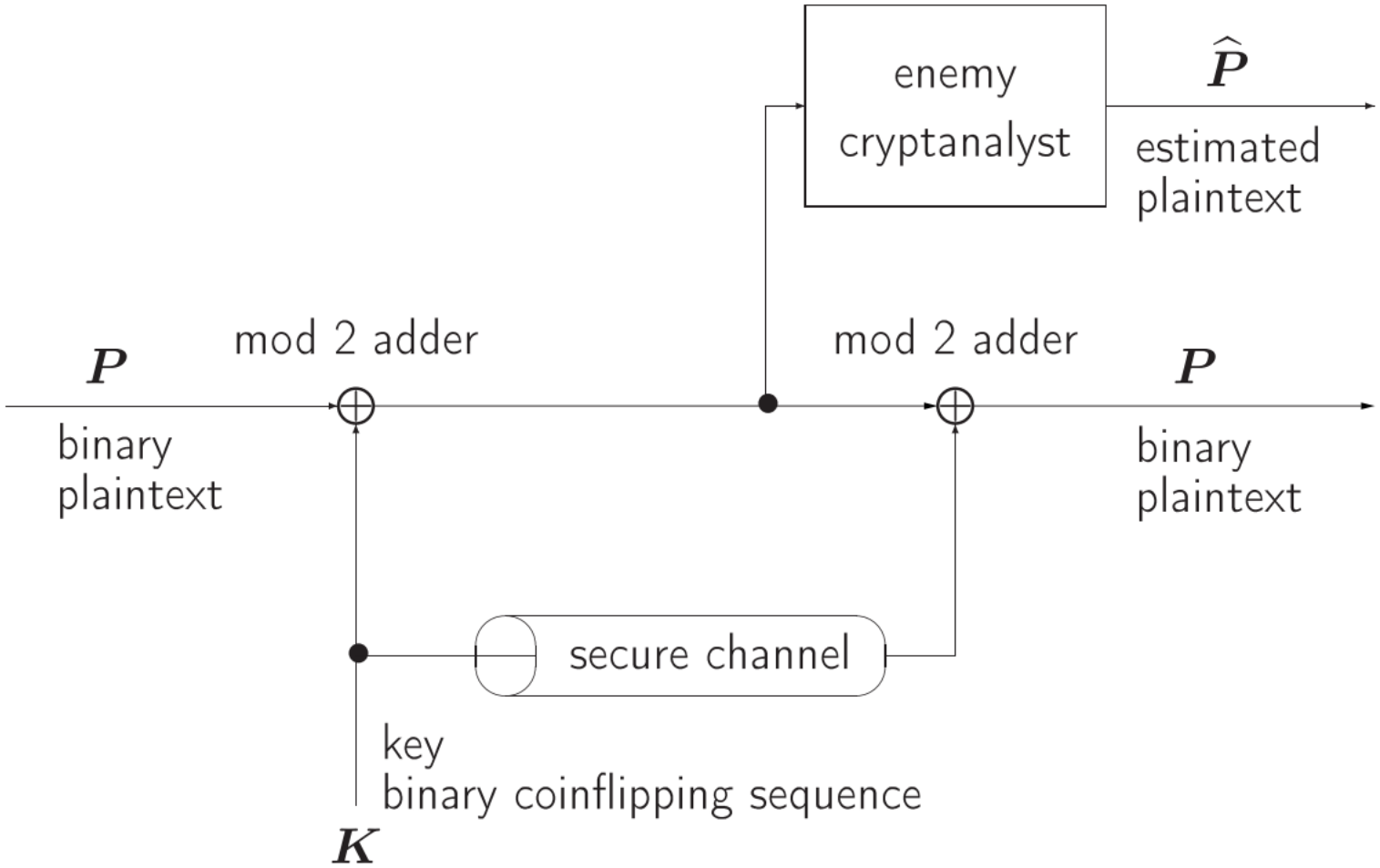
Breaking the Vigenère cipher

The cryptanalyst looks for such repetitions in the ciphertext. In our example we find the repeated string TEBLBP:

plaintext	FORWOODSTOCKMYFRIENDOFFRIENDS
key	THOMPSONTHOMPSONTHOMPSONTHOMP
ciphertext	..............TEBLBP..TEBLBP.

LUND UNIVERSITY

The Vernam cipher



Perfect secrecy

Shannon defined a cryptosystem to provide *perfect secrecy* if the plaintext and the ciphertext are independent random variables.

For such systems we will obtain no information at all about the plaintext by observing only the ciphertext. We might do as well just by guessing the plaintext without observing the ciphertext and by doing so trust our luck!

LUND UNIVERSITY

LUND
UNIVERSITY