CS402

Cryptography: studies how to communicate messages in a way that is secure from interference from third parties called adversaries.

1. Caeser cipher (used by Julius Caeser 100 BC – 44 BC)

YGNEQOCVQETARVQITCRJA

This cipher text was produced by shifting letters according to the rule

Plain: 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

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

The plain text

WELCOMETO.....

2. HSBC Secure key (currently used by online customers)

- A "calculator" is issued to the customer.
- The customer enters their secret 4-digit PIN, and the calculator produces a time dependent 6-digit number.
- The HSBC web page asks the customer for some of those six digits in order to proceed with online banking.

This two-factor authentication uses number theory.

3. Enigma machine (WW2)

German military communicated using an Enigma machine: the operator input a letter of plaintext, and the machine outputs the corresponding letter of ciphertext. Unlike the Caesar cipher, a given plaintext letter corresponds to different ciphertext letters depending on its position in the plaintext message.

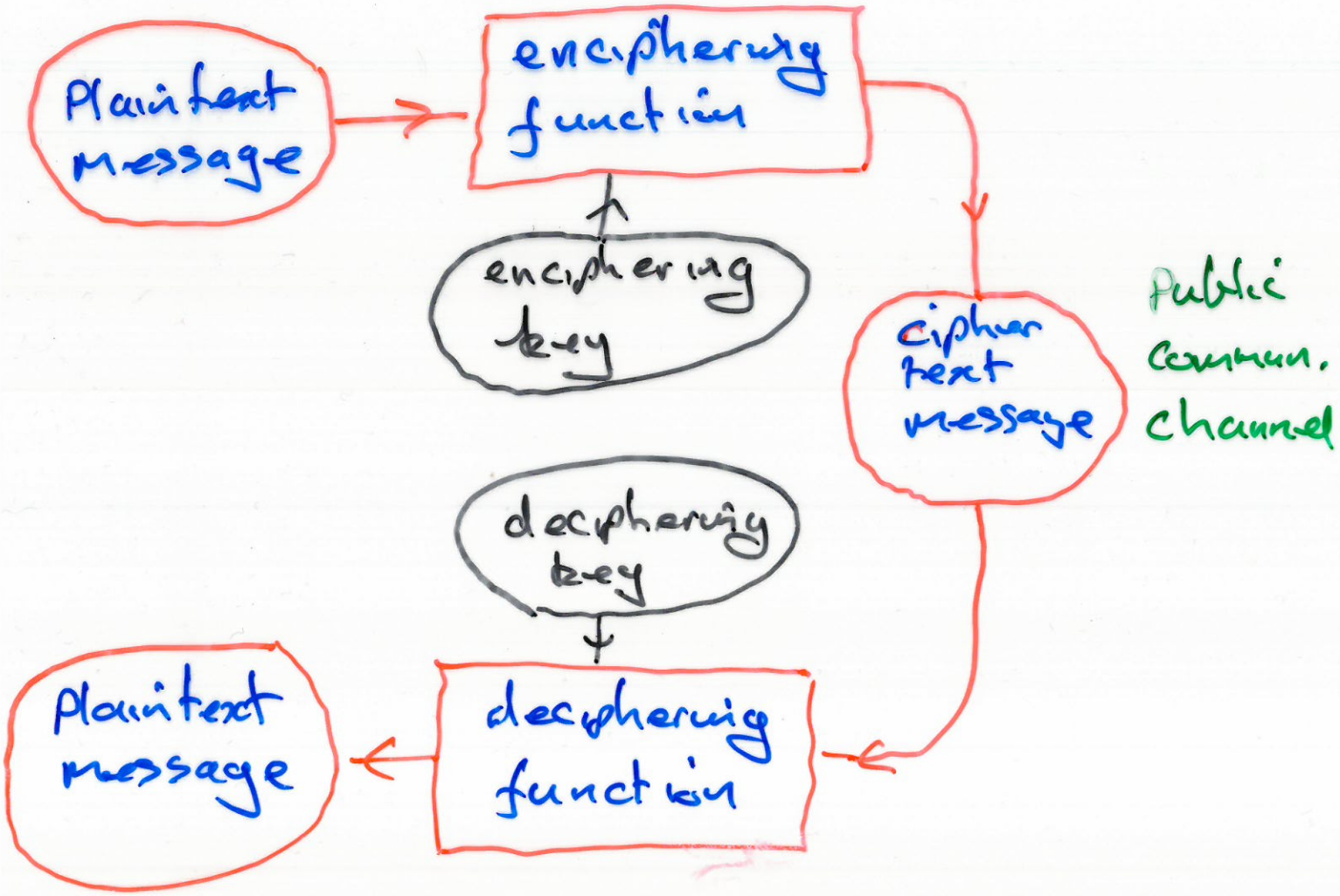
Text book: Cryptography, An Introduction (Third Edition) by Nigel Smart.
Available as a free online book.

Aim: Cover enough of the book so that interested students have enough basis to continue reading on their own.

Preparation: Install Python on your laptop or learn how to start Python in the Computing lab in Aras de Brün.

Assessment: - 70% based on end-of-semester exam. The exam will be based on the problem sheet.
30% base on three online homeworks.

Model for a generic cryptosystem



Kerckhoff's Principle (mid 1800s)

Adversary knows all details of the enciphering / deciphering functions. But the adversary does not know the enciphering/deciphering keys