wdpi eexyv ars lfxek

Capstone project

Early ciphers: Project description

Online at http://bit.ly/vhdl101-10a

José Manuel Martins Ferreira | josemmf@usn.no

Professor | Fakultet for Teknologi, Naturvitenskap og Maritime Fag | https://www.usn.no

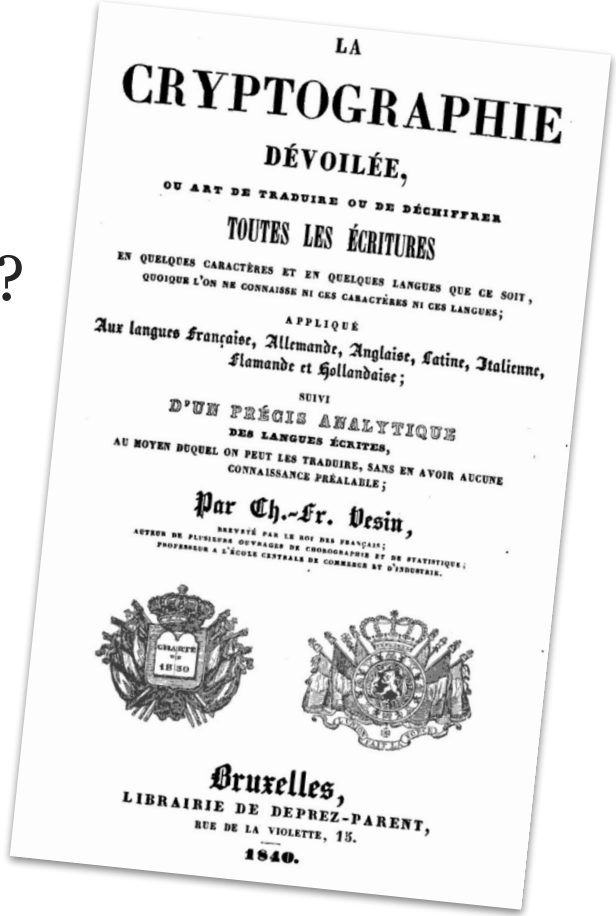
Learning outcomes

After watching this presentation you should be able to:

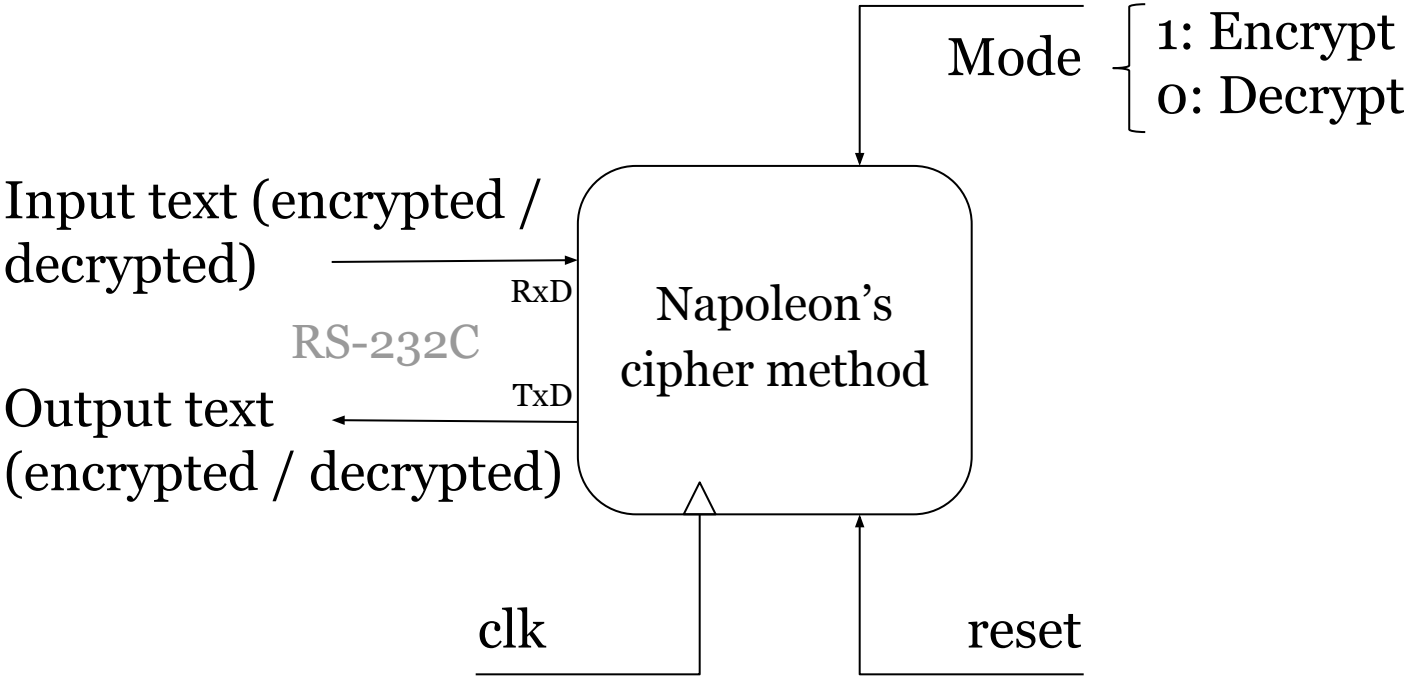
- Explain the functional requirements of the proposed coursework
- Identify the main design tasks and set up a plan for the development work

Early cryptography

- Distinction between code and cipher?
- Napoleon's use and misuse of cryptography: http://bit.ly/2qY5Qtd
- We will use a variant of what is presented in chapter 4 of *La cryptographie dévoilée*, 1840 (pp. 43-63): http://bit.ly/2YVhm54

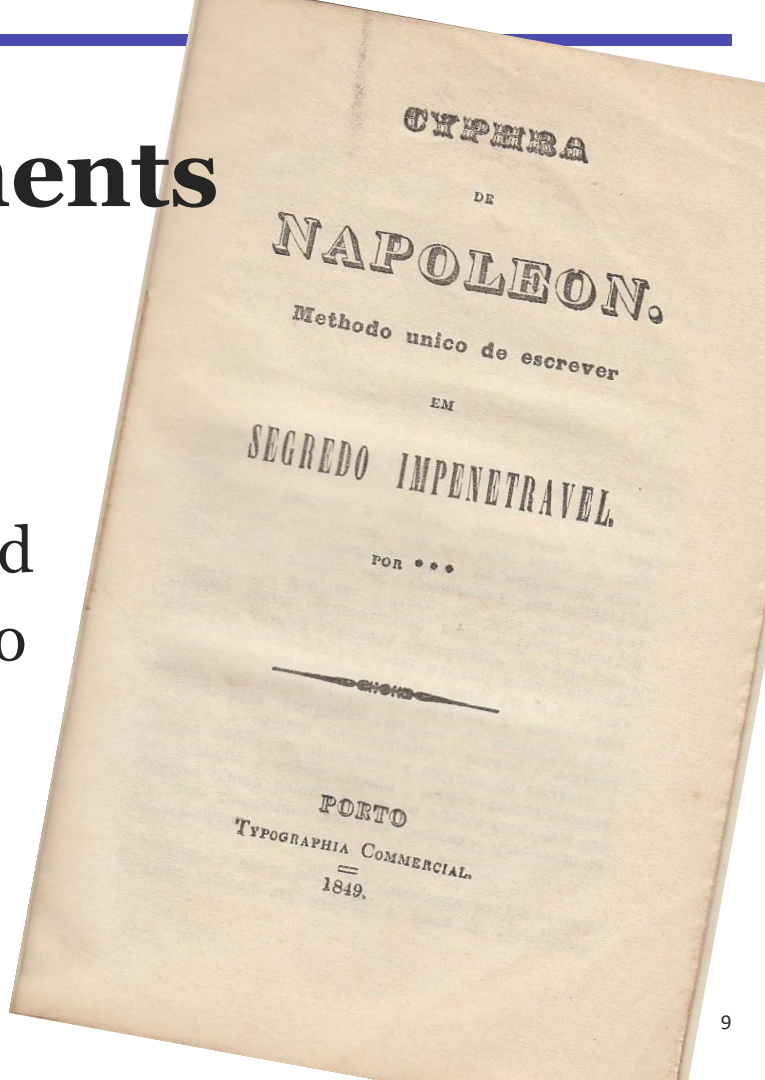

LA
CRYPTOGRAPHIE
DÉVOILÉE,
OU ART DE TRADUIRE OU DE DÉCHIFFRER
TOUTES LES ÉCRITURES
EN QUELQUES CARACTÈRES ET EN QUELQUES LANGUES QUE CE SOIT,
QUOIQUE L'ON NE CONNAISSE NI CES CARACTÈRES NI CES LANGUES;
APPLIQUÉ
Aux langues Française, Allemande, Anglaise, Latine, Italienne, Flamande et Hollandaise;
SUIVI
D'UN PRÉCIS ANALYTIQUE
DES LANGUES ÉCRITES,
AU MOYEN DUQUEL ON PEUT LES TRADUIRE, SANS EN AVOIR AUCUNE CONNAISSANCE PRÉALABLE;
Par Ch.-Fr. Vesin,
BREVETÉ PAR LE ROI DES FRANÇAIS;
AUTEUR DE PLUSIEURS OUVRAGES DE CHRONOGRAPHIE ET DE STATISTIQUE;
PROFESSEUR A L'ÉCOLE CENTRALE DE COMMERCE ET D'INDUSTRIE.
Bruxelles,
LIBRAIRIE DE DEPREZ-PARENT,
RUE DE LA VIOLETTE, 15.
1840.

Overview


Mode
1: Encrypt
0: Decrypt
Input text (encrypted / decrypted)
RxD
RS-232C
TxD
Output text (encrypted / decrypted)
Napoleon's cipher method
clk
reset

Functional requirements

- Consider the 26 letters of the English alphabet
- The key will be hard programmed (FPGA reprogramming needed to modify it)

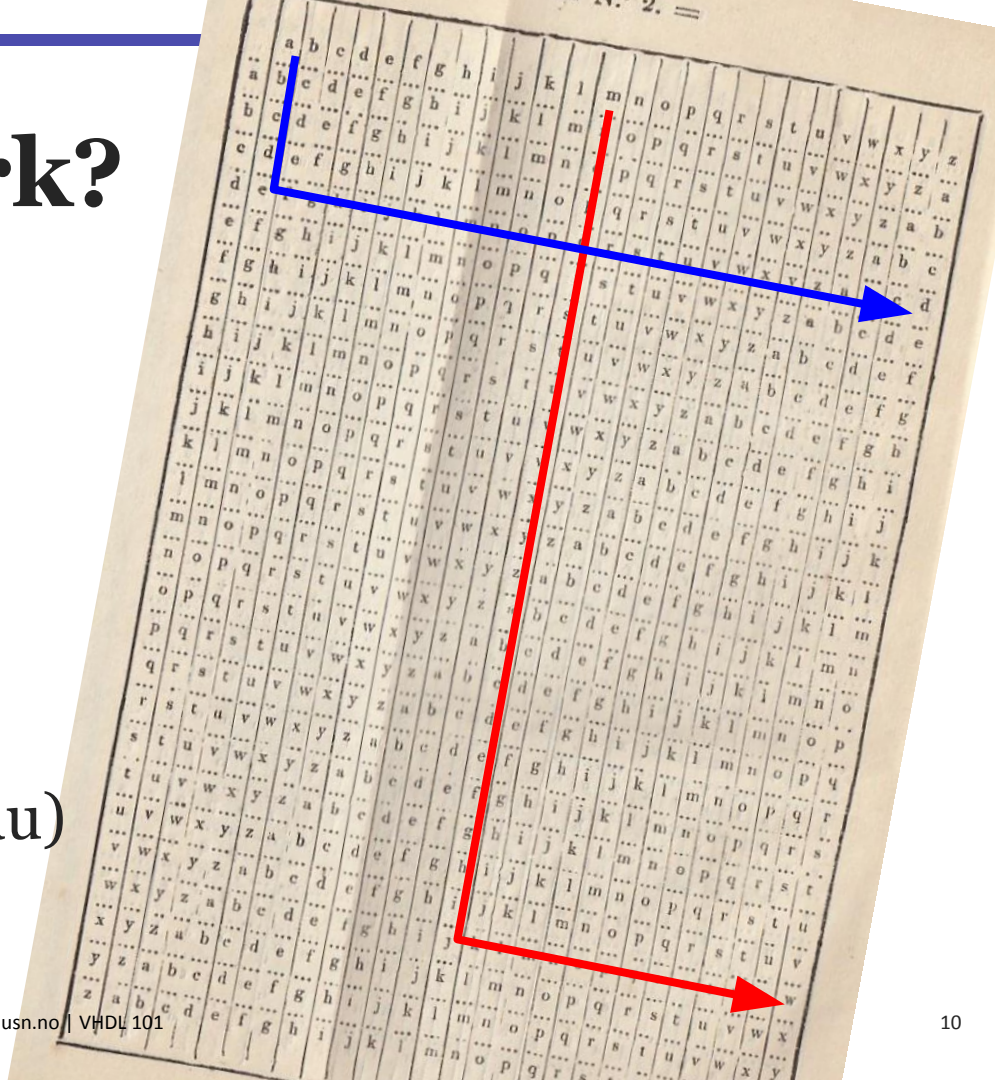


How does it work?

```
Make every day count
|||| ||||| ||| |||||
Jean Jacqu esR ousse
```

```
wdpi eexyv ars lfxek
```

(key: Jean-Jacques Rousseau)



Tasks

FSMD implementation

- Start by designing a data path architecture (data units needed and their interconnection)
- Represent an ordered sequence of actions, and schedule them into ASMD chart states
- Create the VHDL project in Vivado comprising all design files and test benches

Software implementation

- Build a high-level representation of your solution
- Develop the corresponding C / C++ descriptions
- Use Vivado / SDK to create the platform and run your application

IP implementation

- If your coursework assignment asks for an implementation in the form of an IP block, adapt the previous work in order to deliver this solution as well
- Whatever the implementation technology, make sure that you build the necessary test benches to enable appropriate design verification