**Master Electronique, énergie électrique, automatique**
**Parcours** MiSCIT: Master In Systems, Control and Information Technologies

# Security of Networks: Homeworks

Jean-Marc THIRIET

jean-marc.thiriet@univ-grenoble-alpes.fr

http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/miscit/miscit_en.html

# Exercise 0

- exercise 1.1
- 10110
- 11011
- 11001
- Provide the parity (even parity) bits both horizontically and vertically
- 1.2 A receiver receives (even parity) this message
- 111001
- 101110
- 001111
- 001000
- Are there transmission errors? If yes, is it possible to correct the transmission errors? What is the corrected message ? Make an extra comment.

# Exercise 0
# CORRECTION part 1

- exercise 1.1
- 101101
- 110110
- 110011
- **101000**
- 1.2 Provide the parity (even parity) bits both horizontically and vertically
- A receiver receives (even parity) this message of course the receiver has no information about what was the message sent by the transmitter
- 111001 **correct**
- 101110 **correct**
- 001111 **correct**
- 001000 **Uncorrect**
- **There is an error in the last line (last packet of 6 bits), but at this stage we don't know where is this error**

# Exercise 0
# CORRECTION part 2

- **Checking of columns**
- **Cucccc => There is an error second column (c=correct ; u=uncorrect)**
- Are there transmission errors? If yes, is it possible to correct the transmission errors?
- **If we combine both known information, vertically and horizontally, we know which bit is wrong.**
- 111001
- 101110
- 001111
- 001000
- **Because this bit is wrong, we will alternate it, which means change this 0 into 1. We just achieved a correction, without needing a retransmission from the transmitter size**
- What is the corrected message ?
- **The correct message initially sent is so:**
- 111001
- 101110
- 001111
- 001000
- Make an extra comment.
- **What is interesting to notice here is that the wrong bit was not a bit from the data, but a parity bit. This is just to be aware that these security mechanisms are taking account of all the bits in the same way: data bits and control bits… We may also notice that there are actually no transmission errors in the data bits in this example…**

# CORRECTION Ex.1 p. 8 Part 1

- In the ASCII code, the chain “INT” is encoded with the 3 following 7-bits characters (the ASCII code is given as hexadecimal):
- I → 49 **=> 1001001**
- N → 4E **=> 1001110**
- T → 54 **=> 1010100**
- Provide the transmitted message, by adding an even parity both for VRC and LRC. We consider that the parity bit is on the right.
- **10010011**
- **10011100**
- **10101001**
- **10100110**

# CORRECTION Ex.1 p. 8 Part 2

- Same question with an odd parity
- **10010010**
- **10011101**
- **10101000**
- **01011000**

- **! When we compare even and odd parities, all the bits are reverse except the bit at the bottom on the right (intersection between LRC and VRC) !**

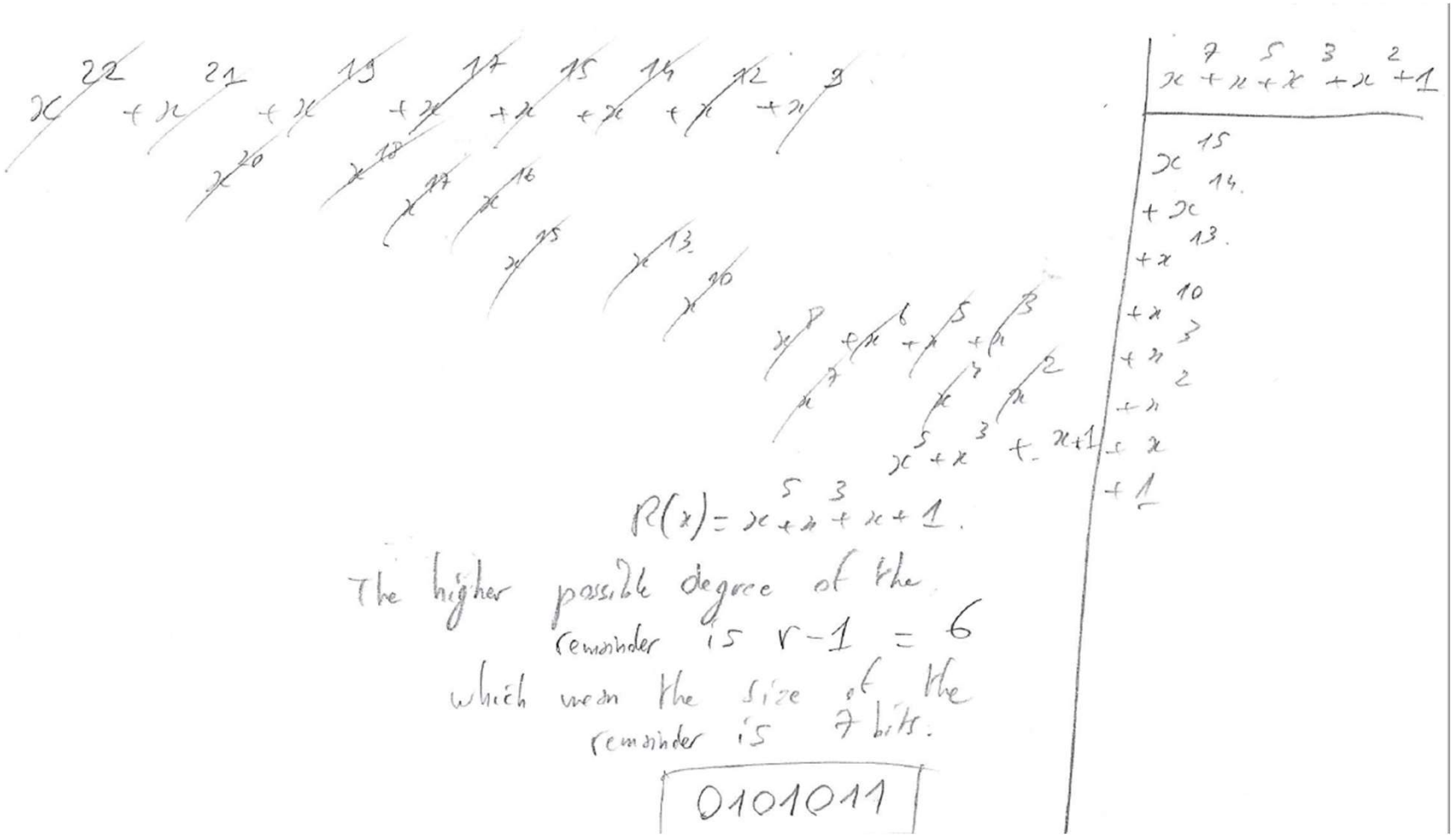
# CORRECTION Ex.2 p. 8 Part 1

- We want to transmit the following message: 11010101 10100100 using the following generator suite: 10101101.
- Give the result of the CRC, explain what is the size of the CRC and why.

# CORRECTION Ex.2 p. 8 Part 2

- $M(x) = x^{15} + x^{14} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^2$
- $G(x) = x^7 + x^5 + x^3 + x^2 + 1$, degree 7
- So $x^r.M(x) = x^{22} + x^{21} + x^{19} + x^{17} + x^{15} + x^{14} + x^{12} + x^9$
- We have now to make the division $x^r.M(x)$ divided by $G(x)$

# CORRECTION Ex.2 p. 8 Part 3



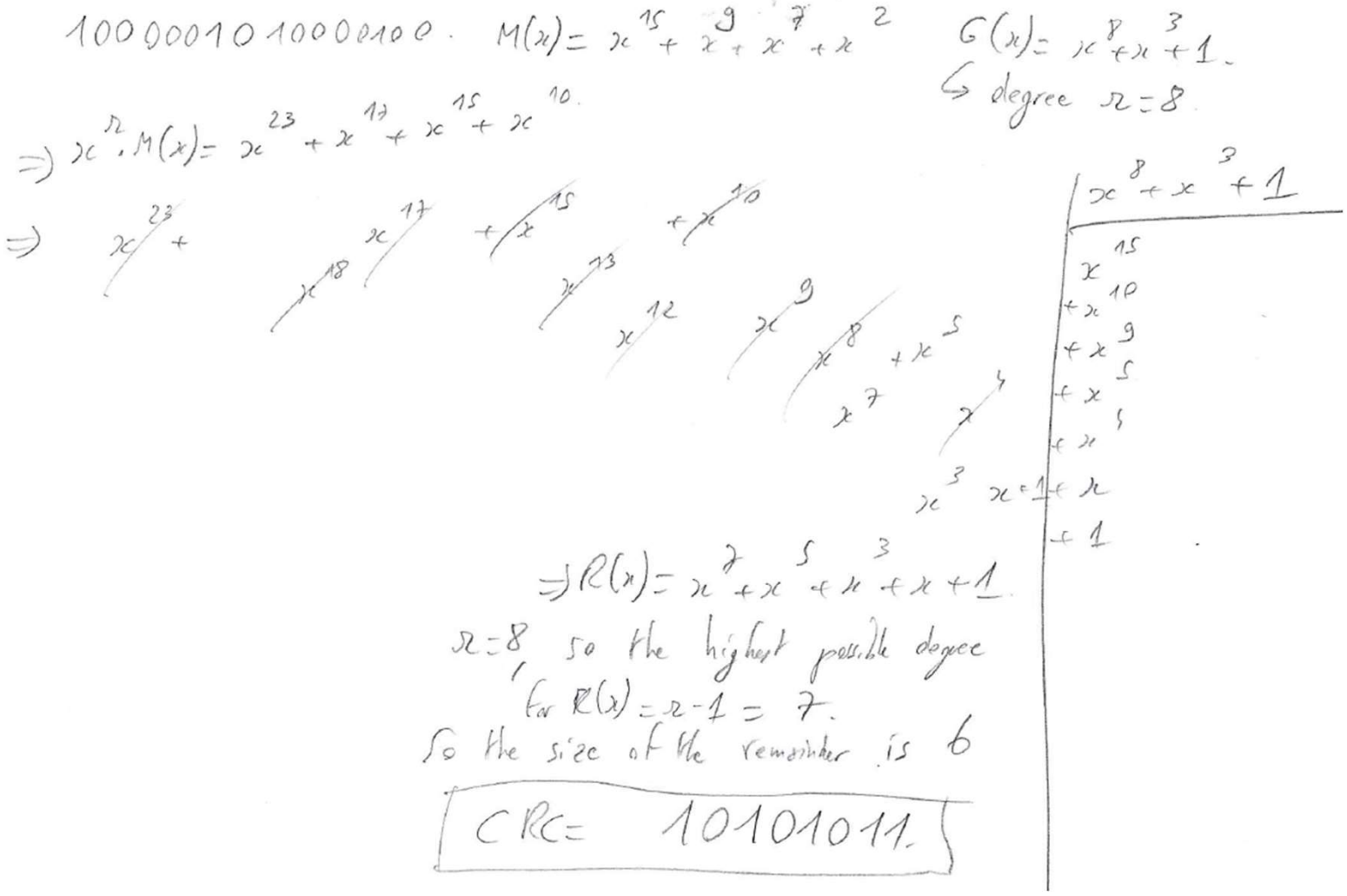
# CORRECTION Ex.3 p. 8

- We want to transmit a message composed of 4 hexadecimal figures: BE85, the (most significant) first bit transmitted is the strong weight of the data,
- BE85 = 1011 1110 1000 0101
- the protection against errors is achieved thanks to 8 odd-parity bits.
- Let's calculate the 8 bits-LRC.
- 10111110
- 10000101
- 11000100
- Give the polynomial form of the message to be transmitted.
- $x^{23} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{15} + x^{10} + x^{8} + x^{7} + x^{6} + x^{2}$
- Give the complete binary suite transmitted to the receiver.
- 101111101000010111000100

# CORRECTION Ex.4 p. 8 Part 1

- We want to transmit the **word** "AB", by supposing that the 8th bit of each character is in even parity. We consider that the parity bit is on the right.
- Define the content to be transmitted in a binary form.
- “AB”, A is hexa  41, B is hexa 42. ASCII codes are on 7 bits and the 8th bit is in even parity
- A => 10000010
- B => 10000100
- The content to be transmited is 1000001010000100
- Then we will calculate the CRC for the defined binary suite. Calculate the corresponding CRC using $x^8 + x^3 + 1$ as a generator polynomial

# CORRECTION Ex.4 p. 8 Part 2



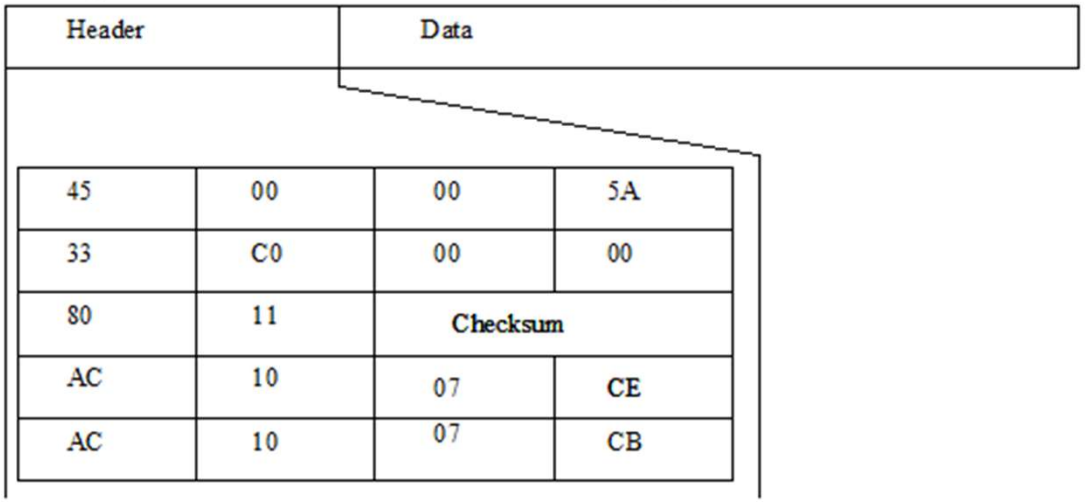
# CORRECTION Ex.5 p. 8 Part 1

- We want to transmit the following 6-bit message: 011011, the first bit transmitted is the bit on the left (strong weight). The suite is transmitted with the following generator polynomial $G(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$
- a) Calculate the remainder obtained by the receiver after division of the received message by G(x).
- The result is $x^7 + x^6 + x^5 + x^3 + x^2 + x$, the size of the remainder is 12 bits (degree 11) so the remainder is 000011101110
- a) Give the binary suite transmitted with the following generator polynomial:
- 011011000011101110, which corresponds to the frame T(x) sent by the transmitter
- c) We suppose that because of a transmission error, the first bit of the CRC transmitted is alternated, give the polynomial value of the remainder R(x) calculated by the receiver.
- It means the receiver receives 011011100011101110. On the receiver side, we divide T(x) / G(x) and the remainder is: $x^{11}$ which is <> 0, which means the frame T has not been received well by the receiver

# CORRECTION Ex.6 p. 4 Part 1

- Exercise 6, page 4 in the textbook

A packet is constituted of a 20-byte header and some data following the structure below:




| | | | |
|---|---|---|---|
| 45 | 00 | 00 | 5A |
| 33 | C0 | 00 | 00 |
| 80 | 11 | Checksum | |
| AC | 10 | 07 | CE |
| AC | 10 | 07 | CB |

Bytes 11 and 12 correspond to the checksum and the header.
Bytes 13 to 16 represent the hexadecimal address of the transmitter.
Bytes 17 to 20 represent the hexadecimal address of the receiver.

a) Calculate the checksum,
b) Determine IP source and destination addresses in a decimal notation

# CORRECTION Ex.6 p. 4 Part 2

- Calculate the checksum
- 4500 + 005A + 33C0 + 0000 + 8011 + AC10 + 07CE + AC10 + 07CB
- 455A + 33C0 + 8011 + B3DE + B3DB
- 791A+133EF + B3DB
- 1AD09 + B3DB = 260E4
- Then we sum the carry: 60E4 + 2 = 60E6
- Then we should reverse, we can do it directly (0 is the reverse of F, 1 from E, 2 from D …, 7 from 8)
- Or we can use the binary form
- 60E6 = 0110 0000 1110 0110
- The reverse is 1001 1111 0001 1001 = 9F19
- So the Cheksum is 9F19

# CORRECTION Ex.6 p. 4 Part 3

- Determine IP source and destination addresses in a decimal notation
- IP source AC1007CE =>
  - ACh corresponds to 172d
  - 10h corresponds to 16d
  - 07h corresponds to 7d
  - CEh corresponds to  206d
- So the IP source is 172.16.7.206
- With the same strategy the IP destination AC1007CB will corresponds to 172.16.7.203

# Homework 3: Risk analysis (1/5)

- Per teams of 4 people, take an example of a company
  - Company in which you will spend your training period, for example
- Achieve an analysis of computer risks
  - Confidentiality
  - Integrity
  - …
- Do some assumptions for each of theses risks
  - Occurrence frequency
  - Consequences (severity)
- Try to give a cost for each of these risks

# HW3 (2/5) : Group organisation

- Grp 1:  Naboulsi, Zeinab (rapp),
- Grp 2 : Sleiman, Farooq (rapp)
- Grp 3 : Mahmood, Liaman (rapp)

# HW3 (3/5) : Steps and deadlines

- This is a group work
- Each group: 1 Leader (to manage the group), 1 Rapporteur (to give the feedback at the end of the process)
- Each group : To choose/define an example of applications (like hospital, airport, shop, government facilities, embedded system (autonomous car, pacemaker…))

# HW3 (4/5) : Steps and deadlines

- Based on the application chosen
  - Make a risk analysis (3 situations)
  - Try to give some indicators
  - Prepare an action plan

# HW3 (5/5) : Expected result

- Presentation (as slides) to be achieved next class: 3rd October done by the rapporteur: 4 slides for a 5-minute presentation
  - 1. Composition of the group, roles, choice of the « application »
  - 2. Risk analysis (3 situations max)
  - 3. Action plan (priorities for the setting of actions to resolve (or decrease) the risks) on the identified situations
  - 4. Explaination of how the group worked
- Slides to be sent to me 2nd October, 8pm at last

# Homework 4: Publication

- Objectives
  - To "cultivate" oneself about security (technology watch)
  - Write a professional document that can complement a CV
- How do you do it?
  - Read articles, websites, make an "analysis" of them (list, your relative notes, etc.).
  - Write a personal "synthesis", your vision based on what you have read.
- Deadlines
  - For Monday, September 30th, 2024, 8.00 pm : Send me
    - The choice of your subject
  - By Monday, 25th November 2024, 8 p.m., latest deadline
    - 1 electronic version of the publication
    - jean-marc.thiriet@univ-grenoble-alpes.fr
- We place ourselves in a professional framework: no delay will be allowed

# Homework 4: Organization of the publication

- The publication should be presented as a 4 to 6 page report respecting the IEEE format, in the spirit of a potential publication
- Title
- Abstract
- Main part (synthesis) written by YOU (not copy-pasted !)
  - State of the art
  - Comparison of existing solutions
  - Type of applications there are used for (more research-oriented at the moment, wide spread existing applications)
  - Trends for the future
  - …
- Bibliographical and “webographic” references
- Possibly extra appendices (interesting documents you may have found), outside the actual memoir

- Each one will have to carry out this « synthesis work » on the basis of readings (books, journals, Internet) and/or from her/his own experience, gained during the practical part of the academic project, for instance, or from past experiences (training periods…)

# Homework 4, potential Subjects

1. Proposal for a network/computer security policy for a company
2. Security protocols, secure architecture through VPN
3. Secure IoTs?
4. Safety industrial networks: ASI safety at works, Profisafe, CanOpenSafe…
5. Security aspects in the field of industrial networks: challenges ? Solutions ?
6. Cyber-security of drones
7. Industrial IoT
8. Telecom, Mobile phone protocoles, security aspects
9. Cloud environment, security challenges
10. Other idea?