



Digitally signed by  
Library TUM  
Reason: I attest to the  
accuracy and integrity  
of this document

# UNIVERSITATEA TEHNICĂ A MOLDOVEI

## METODE CRIPTOGRAFICE DE PROTECȚIE A INFORMAȚIEI

### Partea I

#### CIFRURI SIMETRICE CLASICE *Indicații didactico-metodice*

| <b>k</b> | <b>m</b>     | <b>k</b> | <b>m</b>     |
|----------|--------------|----------|--------------|
| <b>1</b> | <b>26047</b> | <b>6</b> | <b>71592</b> |
| <b>2</b> | <b>15936</b> | <b>7</b> | <b>60481</b> |
| <b>3</b> | <b>04825</b> | <b>8</b> | <b>59370</b> |
| <b>4</b> | <b>93714</b> | <b>9</b> | <b>48269</b> |
| <b>5</b> | <b>82603</b> | <b>0</b> | <b>37158</b> |

Chișinău  
2013

**UNIVERSITATEA TEHNICĂ A MOLDOVEI  
FACULTATEA INGINERIE ȘI MANAGEMENT  
ÎN ELECTRONICĂ ȘI TELECOMUNICAȚII  
CATEDRA TELECOMUNICAȚII**

**METODE CRIPTOGRAFICE DE PROTECȚIE A  
INFORMAȚIEI**

**Partea I**

**CIFRURI SIMETRICE CLASICE**  
*Indicații didactico-metodice*

**Chișinău  
UTM  
2013**

Indicațiile didactico-metodice la disciplina *Teoria transmisiunii informației* sunt dedicate analizei metodelor contemporane de protecție a informației în sistemele de comunicații digitale.

Indicațiile didactico-metodice sunt propuse studenților UTM la profilul 525 – *Electronică și comunicații*, specialitatea *Teleradiocomunicații*, pentru ambele forme de învățământ.

Autori: conf., dr. **I. CHIȚUL**  
conf., dr. **S. ANDRONIC**  
conf., dr. **N. BEJAN**  
conf., dr. **L. NEMERENCO**  
conf., dr. **P. NISTIRIUC**

Recenzent: conf., dr. **V. MOROZOV**

Redactor coordonator: conf., dr. **I. CHIȚUL**

Redactor: **Eugenia BALAN**

---

|                          |                             |
|--------------------------|-----------------------------|
| Bun de tipar 19.02.13    | Formatul hârtiei 60x84 1/16 |
| Hârtie ofset. Tipar RISO | Tirajul 50 ex.              |
| Coli de tipar 5,75       | Comanda nr.16               |

---

UTM, 2004, Chișinău, bd. Ștefan cel Mare și Sfânt, 168  
Secția Redactare și Editare a UTM  
2068, Chișinău, str. Studenților 9/9

© UTM, 2013

## CUPRINS

|  |    |
|--|----|
| 1. CIFRURI SIMETRICE CLASICE.....  | 3  |
| 1.1. Cuvânt înainte.....   | 3  |
| 1.2. Noțiuni de bază și definiții.....   | 5  |
| 1.2.1. Tipuri de amenințări asupra securității<br>sistemului.....  | 5  |
| 1.2.2. Servicii și mecanisme ale securității<br>informaționale .....   | 7  |
| 1.2.3. Criptografia. Noțiuni de bază.....  | 11 |
| 1.3. Cifrurile simetrice clasice .....   | 24 |
| 1.3.1. Cifrurile de substituție .....  | 25 |
| 1.3.1.1. Cifrurile de substituție monoalfabetice.....  | 25 |
| 1.3.1.2. Criptoanaliza cifrurilor monoalfabetice de<br>substituție.....  | 40 |
| 1.3.1.3. Cifrurile polialfabetice .....  | 45 |
| 1.3.1.4. One-time pad (cifrul Vernam) .....  | 65 |
| 1.3.2. Cifruri de transpoziție .....   | 65 |
| ANEXE. Bazele matematice ale criptografiei. Partea 1..   | 72 |
| Anexa A. Aritmetica modulară.....  | 72 |
| 1. Noțiuni de bază .....   | 72 |
| 1.1. Operațiile în $Z_N$ .....   | 75 |
| 1.2. Inversia.....   | 79 |
| 1.3. Operații cu matrice în $Z_N$ .....  | 83 |
| Anexa B. Algoritmul Euclid de determinare<br>a celui mai mare divizor comun și<br>inversa multiplicativă ..... | 86 |
| Bibliografie .....   | 90 |

## BIBLIOGRAFIE

1. Алферов А.П. и др. Основы криптографии. – М.: Гелиос АПВ, 2005. – 478 с.
2. Бабаш А.В., Шанкин Г.П. Криптография. – М.: Солон-Пресс, 2007. – 512 с.
3. Брассар Ж. Современная криптология. М.: Полимед., 1999. – 175 с.
4. Введение в криптографию / Под ред. Яценко В.В. – М.: МНЦМО, 2000. - 288 с.
5. Грибунин В.Г. и др. Цифровая стенография. – М.: Солон-Пресс, 2002. – 272 с.
6. Жельников В. Криптография от папируса до компьютера. – М.: АБФ, 1996. – 334 с.
7. Кан Д. Взломщики кодов / Пер. с англ. – М.: Центрполиграф, 2000. – 473 с.
8. Конахович Г.Ф. и др. Защита информации в телекоммуникационных системах. – К.: МК-Пресс, 2005. - 279 с.
9. Сидельников В.М. Теория кодирования. – М.: Изд. МГУ, 2006. – 285 с.
10. Сمارт Н. Криптография / Пер. с англ. – М.: Техносфера, 2005. – 525 с.
11. Ван Тилберг Х.К.А. Основы криптологии / Пер. с англ. – М.: Мир, 2006. – 476 с.
12. Фергюсон Н., Шнайер Б. Практическая криптография. / Пер. с англ. – Вильямс, 2005. – 424 с.
13. Шнайер Б. Прикладная криптография, 2-е изд. / Пер. с англ. – М.: Триумф, 2002. – 816 с.

14. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Пер. с англ. – СПб.: Питер, 2003. – 368 с.
15. Bodean Gh.C. Coduri nonbinare corectoare de erori. – Chişinău: UTM, 2010. – 544 p.
16. Kahn D. The Codebreakers, Macmillan, N.Y., 1967, p.473.
17. Meneres A.J., van Oorschot P.C., Vanstone S.A. Handbook of applied cryptography, 1996, p.794.
18. Mollin R.A. Codes. The guide to secrecy from Ancient to modern times. Chapman & Hall / CRC, 2005, p.635.
19. Mollin R.A. An introduction to cryptography. 2-nd ed./ Chapman & Hall / CRC, 2007, p.413.
20. Shannon C.E. Communication Theory of Secrecy Systems, Bell Syst. Techn. J., vol. 28, October, 1949, pp. 656-715.
21. Stallings W/ Cryptography and network security. Principles and practices. 4-th ed., Prentice Hall, 2005, p.592.
22. Stamp M., Low R.M. Applied cryptanalyses. John Wiley & Sons, 2007, p.425.