

### **- Laboratorul 3 -**

#### *One Time Pad (OTP), sisteme de criptare istorice, Enigma*

**Disclaimer:** Pe parcursul acestui curs/laborator vi se vor prezenta diverse noțiuni de securitate informatică, cu scopul de a învăța cum să securizați sistemele. Toate noțiunile și exercițiile sunt prezentate în scop didactic, chiar dacă uneori se presupune să gândiți ca un adversar. Nu folosiți aceste tehnici în scopuri malițioase! Acestea pot avea consecințe legale în cazul comiterii unor infracțiuni, pentru care **deveniți pe deplin răspunzători!**

#### **1. One Time Pad (OTP)**



Reamintiți-vă cum funcționează sistemul de criptare *One Time Pad (OTP)*.



Răspundeți la următoarele cerințe:

1. Primiți mesajul criptat următor, în format Base64:

```
o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM8Obhlp3vviAVuBbiOtCSz6husBWqhfF0Q  
/8EZ+6il9KygD3hAfFgnzyv9w==
```

Știți despre acesta că a fost criptat cu cheia secretă următoare, reprezentată în hex:

```
ecb181a479a6121add5b42264db9b44b4b48d7d93c62c56a3c3e1aba64c7517a90ed44f8919484b6ed8a  
cc4670db62c249b9f5bada4ed474c9e4d111308b614788cd4fbdcl1e949c1629e12fa5fdbd9
```

Decriptați. Care este mesajul clar primit?

2. Există o cheie care ar fi decriptat același text criptat de la pct.1 în textul clar următor?  
Care este această cheie? (Atentie! Nu se folosesc diacritice.)

*Orice text clar poate obținut dintr-un text criptat cu OTP dar cu o alta cheie.*

3. Ce impact are refolosirea cheii de la pct.1 pentru o altă criptare?

#### **2. Sisteme de criptare istorice**



Citiți despre sistemele de criptare istorice și experimentați cu resursele disponibile online [1-2].

1. Alegeți un sistem istoric de criptare care folosește *metoda substituției*. Dați un exemplu de criptare și un exemplu de decriptare, explicând cum funcționează. Ce puteți spune despre securitatea sistemului de criptare? Ce tehnici de criptanaliză ați putea folosi pentru a sparge sistemul?
2. Alegeți un sistem istoric de criptare care folosește *metoda transpoziției*. Dați un exemplu de criptare și un exemplu de decriptare, explicând cum funcționează. Ce puteți spune despre securitatea sistemului de criptare? Ce tehnici de criptanaliză ați putea folosi pentru a sparge sistemul?

### 3. Analiza de frecvență



Puteți citi mai multe despre *analiza de frecvență* online [3-4].



Textul următor este criptat cu un sistem de substituție monoalfabetic:

ENHFJ EWK LML EOJ GDJ BMONKC PMCG YEPMAC FOVQGMROEQDHF FMAQNJ. CHWFJ GDJHO HWUJWGHMW HW 1978, GDJV DEUJ EG MWFJ LJJW FENNJK HWCJQEOELNJ, EWK DEUJ LJJW GDJ CALXJFG MY WAPJOMAC KHUMOFJC, GOEUJNC, EWK GMOPJWGC. HW GDJ JWCAHWR VJEOC, MGDJO FDEOEFJGOC DEUJ XMHWJK GDJHO FOVQGMROEQDHF YEPHNV. GDJOJC JUJ, GDJ QECCHUJ EWK CALPHCCHUJ JEJCKOMQQJO, PENNMOV GDJ PENHFHMAC EGGEFTJO, EWK GOJWG, GOACGJK LV ENN, XACG GM WEPJ E YJB. BDHNJ ENHFJ, LML, EWK GDJHO JSGJWKJK YEPHNV BJOJ MOHRHWENN ACJK GM JSQNEHW DMB QALNHF TJV FOVQGMROEQDV BMOTC, GDJV DEUJ CHWFJ LJFMPJ BHKJNV ACJK EFOMCC MGDJO CFHJWFJ EWK JWRHWJJOHWR KMPEHWC. GDJHO HWYNAJWFJ FMWGHWAJC GM ROMB MAGCHKJ MY EFEKJPHE EC BJNN: ENHFJ EWK LML EOJ WMB E QEOG MY RJJT NMOJ, EWK CALXJFG GM WEOOEGHUJC EWK UHCAEN KJQHFGHMWC GDEG FMPLHWJ QJKERMV BHGD HW-XMTJC, MYGJW OJYNJFGHWR MY GDJ CJSHCG EWK DJGJOMWMOPEGHUJ JWUJHOMWPJWGC HW BDHFD GDJV BJOJ LMOW EWK FMWGHWAJ GM LJ ACJK. PMOJ GDEW XACG GDJ BMONKC PMCG YEPMAC FOVQGMROEQDHF FMAQNJ, ENHFJ EWK LML DEUJ LJFMPJ EW EOFDJGVQJ MY KHRHGEN JSFDEWRJ, EWK E NJWC GDOMARD BDHFD GM UHJB LOMEKJO KHRHGEN FANGAOJ. I.KAQMWG EWK E.FEGGEQEW FOVQGMFMAQNJ

Folosiți analiza de frecvență ca să determinați textul clar. Acesta este în limba engleză.



Căutați online sursa textului și citiți povestea.

### 4. Sistemul de criptare mecanic Enigma



Vizualizați video-ul [5] ca să înțelegeți cum funcționează mașina Enigma, apoi folosiți un simulator [6,7] pentru rezolvarea exercițiului.



Parcurgeți următorii pași:

1. Preluati cheia zilei din o carte a codurilor disponibilă online, spre exemplu la [8].
2. Setati cheia zilei în simulatorul Enigma.
3. Criptați numele dumneavoastră. Ce obțineți?
4. Decriptați textul criptat obținut ca să obțineți numele ca text clar. Cum ați procedat?
5. Puteți da un exemplu de text criptat de aceeași lungime care în mod clar nu ar putea fi criptarea numelui? Cum ați gândit?

### **Referințe bibliografice**

1. S.Singh. *The Black Chamber*. Accesibil la: [http://www.simonsingh.net/The\\_Black\\_Chamber/index.html](http://www.simonsingh.net/The_Black_Chamber/index.html) Ultima accesare: septembrie 2021.
2. DCode. Accesibil la: <https://www.dcode.fr/en> Ultima accesare: septembrie 2021.
3. S.Singh. *The Black Chamber – Mono-alphabetic ciphers*. Accesibil la: [http://www.simonsingh.net/The\\_Black\\_Chamber/monoalphabetic.html](http://www.simonsingh.net/The_Black_Chamber/monoalphabetic.html) Ultima accesare: septembrie 2021.
4. S.Singh. *The Black Chamber – Cracking the substitution cipher*. Accesibil la: [http://www.simonsingh.net/The\\_Black\\_Chamber/crackingsubstitution.html](http://www.simonsingh.net/The_Black_Chamber/crackingsubstitution.html) Ultima accesare: septembrie 2021.
5. World Science Festival. *The Enigma Machine Explained*. Accesibil la: [https://www.youtube.com/watch?v=ASfAPOiq\\_eQ&ab\\_channel=WorldScienceFestival](https://www.youtube.com/watch?v=ASfAPOiq_eQ&ab_channel=WorldScienceFestival) Ultima accesare: septembrie 2021.
6. 101 Computing Net. Enigma Machine Simulator. Accesibil la: <https://www.101computing.net/enigma-machine-emulator/> Ultima accesare: septembrie 2021.
7. Ciphers Machines and Cryptology. *Enigma Simulator*. Accesibil la: <http://users.telenet.be/d.rijmenants/en/enigmasim.htm> Ultima accesare: septembrie 2021.
8. Operation Turing. Accesibil la: <https://operationturing.tumblr.com/> Ultima accesare: septembrie 2021.