Laborator 3

One Time Pad (OTP)

m, k, c de lungime n

$$E_k(m) = m \oplus k = c$$
$$D_k(c) = c \oplus k = m \oplus k \oplus k = m$$

unde

m = mesajul in clar

k = cheia de criptare

c = mesajul criptat

E_k = criptatea mesajului

D_k = decriptarea mesajului

1. Caesar Chiper

substitutie monoalfabetica

k = 3 ⇒ A → D

c_i = (m_i + k) % 26

m = SALUTZ ⇒ c = VDOXWC

---

2. Vigenère Chiper

subtitutie polialfabatic

k = **KING,** A → K, A → I, A → N, A→ G

k = 10, k = 8, k = 13, k = 6

m = **THE SUN AND THE MAN IN THE MOON**

c = DPRY EVNT NBUK WIAO XBUK WWBT

unde : T → 10 → D, H → 8 → P, …

Exercitii

▼ **Exercitiul 1.1**

c = a3dfe4842dcf7f7ffd0b23426ddcc73f2e68a2b71c11ac19485b779a00a27119e284348cf0e6e1969defbe2015b816e23ad092c

k = ecb181a479a6121add5b42264db9b44b4b48d7d93c62c56a3c3e1aba64c7517a90ed44f8919484b6ed8acc4670db62c249b

m = c + k = 4f6e652054696d65205061642065737465207 56e2073697374656d206465206372697074617265207065726566563742073 6 (hex)

hex to ascii: One Time Pad este un sistem de criptare perfect sigur daca este folosit corect.

▼ **Exercitiul 1.2**

m = Orice text clar poate obtinut dintr-un text criptat cu OTP dar cu alta cheie..

m = 4F726963652074657874206 36C617220706F617465206F6274696E75742064696E74722D756E2074657874206372697 07 (hex)

c = o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM8Obhlp3vviAVuBbiOtCSz6husBWqhfF0Q/8EZ+6iI9KygD3hAfF (base64)

c =

a3dfe4842dcf7f7ffd0b23426ddcc73f2e68a2b71c11ac19485b779a00a27119e284348cf0e6e1969defbe2015b816e23ad092c
(hex)

Rescriem m + k = c => k = c + m (operatia inversa lui xor este tot xor)
k =
a39096ed4eaa5f0b987357620eb0a64d0e18cdd668748c762a2f1ef475d6517d8bea40fedd938fb6e98ac65435db648b4aa4f3

▼ **Exercitiul 1.3**

c1 = m1 + k
c2 = m2 + k
c1 + c2 = m1 + m2 (criptarea nu e sigura)

▼ **Exercitiul 2.1**

https://cryptii.com/

- **Caesar:**

m: THE SUN AND THE MAN ON THE MOON, k: 4

c: XLI WYR ERH XLI QER SR XLI QSSR

- **Vigenere:**

m: THE SUN AND THE MAN ON THE MOON, k: **KEY**

c: DLC CYL KRB DLC WEL YR RRI KYSL

▼ **Exercitiul 2.2**

https://cryptii.com/

- **Rail Fence:**

m: THE SUN AND MOON

1	T	.	.	.	S	.	.
2	.	H	.	_	.	U	.
3	.	.	E	.	.	.	N

c: TSAMH U N ONENDO

▼ **Exercitiul 3**

http://scottbryce.com/cryptograms/cgi-bin/cryptograms.pl

```
ALICE AND BOB ARE THE WORLDS MOST
ENHFJ EWK LML EOJ GDJ BMONKC PMCG

FAMOUS CRYPTOGRAPHIC COUPLE. SINCE
YEPMAC FOVQGMROEQDHF FMAQNJ. CHWFJ

THEIR INVENTION IN 1978, THEY HAVE AT
GDJHO HWUJWGHMW HW 1978, GDJV DEUJ EG

ONCE BEEN CALLED INSEPARABLE, AND HAVE
MWFJ LJJW FENNJK HWCJQEOELNJ, EWK DEUJ

BEEN THE SUBJECT OF NUMEROUS DIVORCES,
LJJW GDJ CALXJFG MY WAPJOMAC KHUMOFJC,

TRAVELS, AND TORMENTS. IN THE ENSUING
GOEUJNC, EWK GMOPJWGC. HW GDJ JWCAHWR

YEARS, OTHER CHARACTERS HAVE JOINED
VJEOC, MGDJO FDEOEFGJOC DEUJ XMHWJK

THEIR CRYPTOGRAPHIC FAMILY. THERES EVE,
GDJHO FOVQGMROEQDHF YEPHNV. GDJOJC JUJ,

THE PASSIVE AND SUBMISSIVE
GDJ QECCHUJ EWK CALPHCCHUJ

EAVESDROPPER, MALLORY THE MALICIOUS
JEUJCKOMQQJO, PENNMOV GDJ PENHFHMAC

ATTACKER, AND TRENT, TRUSTED BY ALL,
EGGEFTJO, EWK GOJWG, GOACGJK LV ENN,
```

```
JUST TO NAME A FEW. WHILE ALICE, BOB,
XACG GM WEPJ E YJB. BDHNJ ENHFJ, LML,

AND THEIR EXTENDED FAMILY WERE
EWK GDJHO JSGJWKJK YEPHNV BJOJ

ORIGINALLY USED TO EXPLAIN HOW PUBLIC
MOHRHWENNV ACJK GM JSQNEHW DMB QALNHF

KEY CRYPTOGRAPHY WORKS, THEY HAVE SINCE
TJV FOVQGMROEQDV BMOTC, GDJV DEUJ CHWFJ

BECOME WIDELY USED ACROSS OTHER SCIENCE
LJFMPJ BHKJNV ACJK EFOMCC MGDJO CFHJWFJ

AND ENGINEERING DOMAINS. THEIR
EWK JWRHWJJOHWR KMPEHWC. GDJHO

INFLUENCE CONTINUES TO GROW OUTSIDE OF
HWYNAJWFJ FMWGHWAJC GM ROMB MAGCHKJ MY

ACADEMIA AS WELL: ALICE AND BOB ARE NOW
EFEKJPHE EC BJNN: ENHFJ EWK LML EOJ WMB

A PART OF GEEK LORE, AND SUBJECT TO
E QEOG MY RJJT NMOJ, EWK CALXJFG GM

NARRATIVES AND VISUAL DEPICTIONS THAT
WEOOEGHUJC EWK UHCAEN KJQHFGHMWC GDEG

COMBINE PEDAGOGY WITH IN-JOKES, OFTEN
FMPLHWJ QJKERMRV BHGD HW-XMTJC, MYGJW

REFLECTING OF THE SEXIST AND
OJYNJFGHWR MY GDJ CJSHCG EWK

HETERONORMATIVE ENVIRONMENTS IN WHICH
DJGJOMWMOPEGHUJ JWUHOMWPJWGC HW BDHFD

THEY WERE BORN AND CONTINUE TO BE USED.
GDJV BJOJ LMOW EWK FMWGHWAJ GM LJ ACJK.

MORE THAN JUST THE WORLDS MOST FAMOUS
PMOJ GDEW XACG GDJ BMONKC PMCG YEPMAC

CRYPTOGRAPHIC COUPLE, ALICE AND BOB
FOVQGMROEQDHF FMAQNJ, ENHFJ EWK LML

HAVE BECOME AN ARCHETYPE OF DIGITAL
DEUJ LJFMPJ EW EOFDJGVQJ MY KHRHGEN

EXCHANGE, AND A LENS THROUGH WHICH TO
JSFDEWRJ, EWK E NJWC GDOMARD BDHFD GM

VIEW BROADER DIGITAL CULTURE. Q.DUPONT
UHJB LOMEKJO KHRHGEN FANGAOJ. I.KAQMWG

AND A.CATTAPAN CRYPTOCOUPLE
EWK E.FEGGEQEW FOVQGMFMAQNJ
```