**Laborator 3**

One Time Pad (OTP):

Mesajul criptat in Base64: o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM8Obhlp3vviAVuBbiOtCSz6husBWqhfF0Q/8EZ+6iI9KygD3hAfFgnzyv9w==

Mesajul criptat in hex:

a3dfe4842dcf7f7ffd0b23426ddcc73f2e68a2b71c11ac19485b779a00a27119e284348cf0e6e1969defbe2015b816e23ad092cfa86eb015aa85f17443ff0467eea223d2b2803de101f1609f3caff7

Cheia in hex:

ecb181a479a6121add5b42264db9b44b4b48d7d93c62c56a3c3e1aba64c7517a90ed44f8919484b6ed8a

cc4670db62c249b9f5bada4ed474c9e4d111308b614788cd4fbdc1e949c1629e12fa5fdbd9

Mesajul criptat XOR cheia:

4f6e652054696d6520506164206573746520756e2073697374656d20646520637269707461726520706572666563742073696775722064616361206573746520666f6c6f73697420636f726563742e

Echivalent cu:

One Time Pad este un sistem de criptare perfect sigur daca este folosit corect.

2.

Textul clar in hex: 4F72696365207465787420636C617220706F617465206F6274696E75742064696E74722D756E20746578742063726970746174206375204F545020646172206375206F20616C74612063686569652E

Textul clar in hex XOR mesajul criptat in hex:

ecad8de748ef0b1a857f032101bdb51f5e07c3c37931c37b3c3219ef748215708cf046a18588c1e2f897ca0076ca7f924eb1e6efcb1b905afed5d110228d24049b824cf2d3ec4980219208fa55cad9

1. Refolosirea cheii face ca un atacator să aibă mai multe oportunități de a încerca să decripteze mesajele criptate si creste vulnerabilitatea la atacuri brute force si la criptanaliza. De asemenea, odata aflata cheia toate mesajele criptate cu aceeasi cheie vor fi aflate.

Sisteme de criptare istorice:

1. Cifrul Caesar

Pentru a cripta un mesaj folosind cifrul Cezar, se efectuează o deplasare fixă a fiecărei litere din textul clar cu un număr specific de poziții în alfabet. De exemplu, cu o deplasare de 3 poziții (cifrul Cezar cu cheia 3), cuvântul "HELLO" devine "KHOOR". Folosirea unei aranjari normale a alfabetului, ('A'..'Z', 'a'..'z') duce la spargerea destul de simpla a sistemului prin luarea valorilor pe rand si incercarea lor. Sistemul poate fi facut mai sigur prin rearanjarea alfabetului (65! de posibilitati de aranjare a alfabetului in ordine circulara).

Tehnici de criptanaliză pentru a sparge cifrul Cezar includ:

Bruteforce: Un atacator poate încerca toate cele 25 de deplasări posibile pentru a decripta mesajul. Aceasta este o metodă simplă și eficientă de spargere a cifrului.

Analiza frecvenței literelor: O altă tehnică este să se analizeze frecvența literelor în textul criptat. În limba engleză, anumite litere (cum ar fi E sau T) sunt mai frecvente decât altele. Prin urmărirea acestor frecvențe, un atacator poate ghici deplasarea și decripta mesajul.

Analiza contextului: Dacă un atacator are cunoștințe despre contextul mesajului sau poate prezice conținutul acestuia (de exemplu, "HELLO"), poate face ghiciri informate pentru decriptare.

1. Cifrul Rail Fence

Cifrul Rail Fence (sau Zigzag Cipher) este o metodă de criptare prin transpoziție care implică scrierea mesajului clar în zigzag pe mai multe linii, apoi citirea literelor într-o ordine specifică. Iată cum poți cripta și decripta un mesaj folosind cifrul Rail Fence:

Exemplu de criptare (cifrul Rail Fence):

Pentru a cripta un mesaj, trebuie să alegi un număr de linii (cheia de criptare). De exemplu, pentru cheia 3, mesajul "HELL\OWORLD" este scris astfel:

H . . . O . . . . L . .

. E . L . W . R . . . D . .

. . L . . . O . . . . .

Apoi se citesc literele de la stânga la dreapta pe fiecare linie și se concateneaza. In acest caz, mesajul criptat ar fi "HOLELWRDLO".

Securitatea cifrului Rail Fence este destul de scăzută, deoarece numărul posibil de chei (numărul de linii) este limitat și poate fi încercat destul de ușor prin forță brută. În plus, structura zigzag a mesajului este ușor de observat, ceea ce face ca acest cifru să fie vulnerabil la criptanaliză.

Pentru a sparge cifrul Rail Fence, un atacator poate încerca diferite chei (numere de linii) și observa structura zigzag a mesajului. Dacă se cunoaște lungimea mesajului, se pot face presupuneri cu privire la numărul de linii. De asemenea, analiza frecvenței literelor poate ajuta la ghicirea unor cuvinte comune din mesaj. În general, cifrul Rail Fence este mai potrivit pentru scopuri didactice sau pentru mesaje non-sensibile, dar nu oferă o securitate semnificativă împotriva atacurilor cibernetice avansate.

1. Analiza de frcventa:

Am folosit siteul https://scottbryce.com/cryptograms/

ALICE AND BOB ARE THE WORLDS MOST FAMOUS CRYPTOGRAPHIC COUPLE. SINCE

THEIR INVENTION IN 1978, THEY HAVE AT ONCE BEEN CALLED INSEPARABLE, AND

HAVE BEEN THE SUBJECT OF NUMEROUS DIVORCES, TRAVELS, AND TORMENTS. IN THE

ENSUING YEARS, OTHER CHARACTERS HAVE JOINED THEIR CRYPTOGRAPHIC FAMILY.

THERES EVE, THE PASSIVE AND SUBMISSIVE EAVESDROPPER, MALLORY THE MALICIOUS

ATTACKER, AND TRENT, TRUSTED BY ALL, JUST TO NAME A FEW. WHILE ALICE, BOB, AND

THEIR EXTENDED FAMILY WERE ORIGINALLY USED TO EXPLAIN HOW PUBLIC KEY

CRYPTOGRAPHY WORKS, THEY HAVE SINCE BECOME WIDELY USED ACROSS OTHER

SCIENCE AND ENGINEERING DOMAINS. THEIR INFLUENCE CONTINUES TO GROW

OUTSIDE OF ACADEMIA AS WELL: ALICE AND BOB ARE NOW A PART OF GEEK LORE, AND

SUBJECT TO NARRATIVES AND VISUAL DEPICTIONS THAT COMBINE PEDAGOGY

WITH IN-JOKES, OFTEN REFLECTING OF THE SEXIST AND HETERONORMATIVE

ENVIRONMENTS IN WHICH THEY WERE BORN AND CONTINUE TO BE USED. MORE THAN

JUST THE WORLDS MOST FAMOUS CRYPTOGRAPHIC COUPLE, ALICE AND BOB HAVE

BECOME AN ARCHETYPE OF DIGITAL EXCHANGE, AND A LENS THROUGH WHICH TO VIEW

BROADER DIGITAL CULTURE. Q.DUPONT AND A.CATTAPAN CRYPTOCOUPLE

1. Sistemul de criptatre mecanic Enigma:
2. Am ales cheia zilei 3
3. Am folosit simulatorul <https://cryptii.com/> cu urmatoarele setari:

IV, II, III; 18, 03, 23; bq cr di ej kw mt os px uz gh; DDH

1. Panait Ana Maria -> zwcfl fckvo ewyf
2. zwcfl fckvo ewyf -> panai tanam aria
3. Panait Ana Maria





