Laboratorul 3

Exercitiul 2

1. Am ales sistemul de criptare Atbash, un sistem dezvoltat initial pentru criptarea mesajelor scrise in alfabetul evreiesc, dar car epoate fi modificat pentru a scrie orice fel de mesaj. Acest sistem de criptare ia fiecare litera din alfabet, si o inlocuieste cu cea din pozitia opusa. Adica prima cu ultima, a doua cu penultima etc. Acest sistem a fost folosit inclusiv in Biblie pentru a encifra unele toponime. Fiind un sistem de substitutie, fiecare litera are doar o litera ce o poate substitui. Stiind acest fapt, o metoda eficienta de criptanaliza ar fi analiza de frecventa, deoarece frecventele literelor din mesaj vor fi in continuare aceleasi cu frecventele literelor din mesajul original, deci stiind limba mesajului si astfel frecventele fiecarei litere in acea limba putem descifra mesajul. Nu este un sistem de criptare foarte sigur deoarece necesita foarte putin efort si putere de calcul pentru a fi decriptat.
2. Metoda transpozitiei se refera la metoda de criptare a unui text prin a transpune pozitiile literelor din alfabet, fara a modifica insa literele in sine, practic textul obtinut va fi o permutare a textului initial. Pentru a putea reorganiza literele in ordinea initiala, avem nevoie de cheia folosita in procesul de encodare. Acest tip de cifru este frecvent folosit in asociere cu un sistem de substitutie. Un sistem de acest tip este Rail Fence, in care ne alegem un numar de randuri si scriem textul diagonal pe acele randuri, el putand fi astfel citit pe diagonala. De fiecare data cand ajungem pe ultimul rand, vom relua de jos in sus, cand ajungem inapoi pe primul rand vom relua de sus in jos, practic in zig-zag. Spre exemplu, textul “ text” scris pe patru randuri ar arata astfel:

T

e t

x

Urmatorul pas este sa citim acest text de la stanga la dreapta, rand cu rand, ca si cum ar fi un text normal, si vom obtine textul cifrat “Tetx”. Cheia cifrului este numarul de randuri folosit.

Avand in vedere ca nu putem folosi un numar de randuri mai mare decat lungimea textului, suntem limitati in numarul de chei pe care le putem folosi. Asta inseamna ca un atac de forta bruta poate cu usurinta sa obtina textul original, pur si simplu incercand toate cheile pana la lungimea textului.

Exercitiul 3

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 FDEOEFGJOC DEUJ XMHWJK GDJHO FOVQGMROEQDHF YEPHNV. GDJOJC JUJ, GDJ QECCHUJ EWK CALPHCCHUJ JEUJCKOMQQJO, PENNMOV GDJ PENHFHMAC EGGEFTJO, EWK GOJWG, GOACGJK LV ENN, XACG GM WEPJ E YJB. BDHNJ ENHFJ, LML, EWK GDJHO JSGJWKJK YEPHNV BJOJ MOHRHWENNV 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 QJKERMRV BHGD HW-XMTJC, MYGJW OJYNJFGHWR MY GDJ CJSHCG EWK DJGJOMWMOPEGHUJ JWUHOMWPJWGC 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

Text in limba engleza criptat printr-un procedeu de substitutie monoalfabetic

Acest tip de cifru poate fi decriptat prin analiza de frecventa. Stiind in ce limba este, putem asocia literelor si unor grupuri de litere frecvente, numarandu-le aparitiile in text, si pe baza acestor frecvente le putem asocia o alta litera sau un alt grup de litere ce are aceeasi frecventa in limba textului. Spre exemplu, stim ca in limba engleza litera E este cea mai comuna. Vom inlocui cea mai comuna litera din textul nostru, in acest caz J, cu litera E. A doua cea mai comuna litera din text, G, va fi inlocuita cu a doua cea mai comuna litera din limba engleza, anume T. Astfel obtinem:

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. Z.DUPONT AND A.CATTAPAN CRYPTOCOUPLE

Alice si Bob sunt o pereche de personaje folosita frecvent in discutiile despre criptografie, pentru a semnifica doua personaje ce vor sa transmita un mesaj criptat intre ele. Eve, Mallory si Trent sunt numele cel mai frecvent utilizate pentru a reprezenta pe cineva care vrea sa intercepteze si sa decripteze mesajul.