1. One Time Pad
    1.1. One Time Pad este un sistem de criptare perfect sigur daca este folosit corect.
    1.2. 0xa39096ed4eaa5f0b987357620eb0a64d0e18cdd668748c762a2f1ef475d65 17d8bea40fedd938fb6e98ac65435db648b4aa4f3bb880dc535e5d1a154279e 76478dd703bd92e1519560d103f759c692
    1.3. Daca refolosim cheia, vom putea in continuare decripta respectiva criptare, dar nu vom avea mesajul original deoarece nu am folosit cheia cu care acesta a fost criptat initial.

2. Sisteme de criptare istorice
    2.1. Cifrul Atbash este un tip de cifru monoalfabetic de subsitutie care mapeaza alfabetul pe inversul sau.

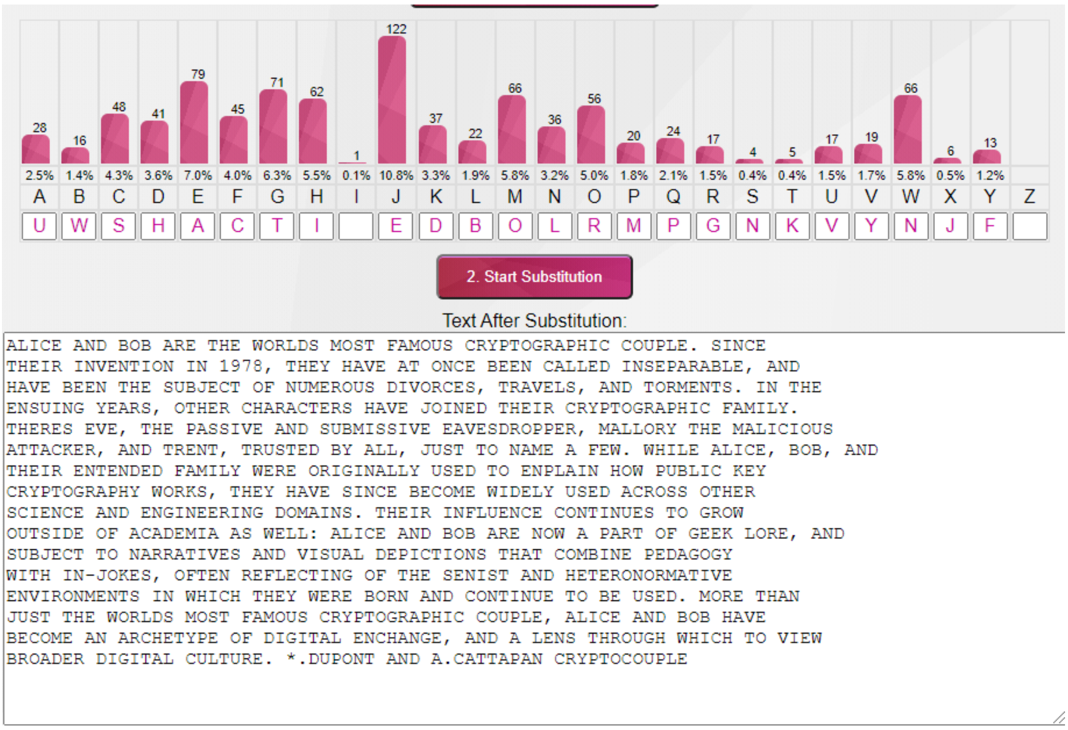
    Text criptat: hvxfirgzgv
    Text decriptat: securitate

    Securitatea este mica deoarece exista 1/26 posibilitati de a “ghici” cheia.
    Se poate analiza frecventa aparitiei cifrelor

    2.2. Folosind un cifru de tip ruta, textul este scris pe un grid cu dimensiuni specificare si apoi citit folosind un model dat de cheie.
    Pentru a ilustra, voi folosi textul: SECURITATE INFORMATICA
    S U T E F M I
    E R A I O A C
    C I T N R T A
    Cheia poate specifica “spirala, in sensul acelor de ceas, incepand din coltul din dreapta sus”. Avem cifrul:
    ICATRNT ICESUTE FMAOIAR
    Acest tip de cifruri au foarte multe chei. Nu toate cheile sunt la fel de bune. Rute alese prost vor lasa prea mult text vizibil sau text care este pur si simplu inversat si astfel vor oferi sansa de a fi decriptate.

3. Analiza de frecventa
    3.1. 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 ENTENDED FAMILY WERE ORIGINALLY USED TO ENPLAIN 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 SENIST 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 ENCHANGE, AND A LENS THROUGH WHICH TO VIEW
BROADER DIGITAL CULTURE. *.DUPONT AND A.CATTAPAN CRYPTOCOUPLE

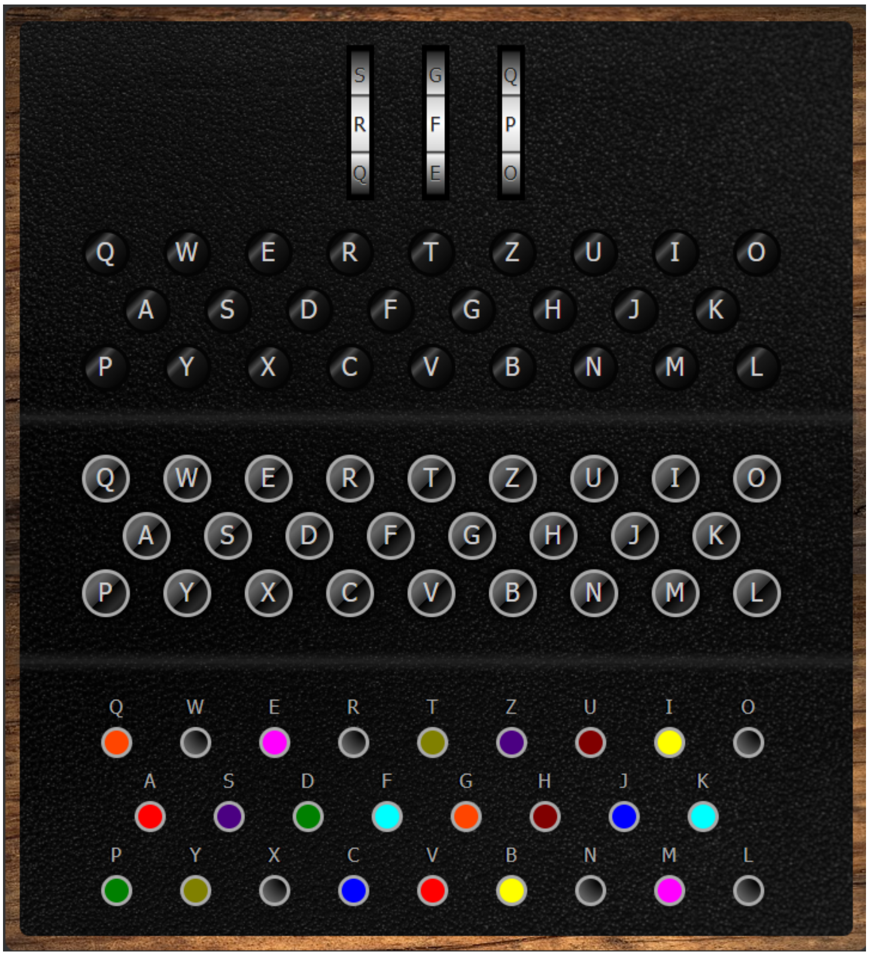


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
28	16	48	41	79	45	71	62	1	122	37	22	66	36	56	20	24	17	4	5	17	19	66	6	13	
2.5%	1.4%	4.3%	3.6%	7.0%	4.0%	6.3%	5.5%	0.1%	10.8%	3.3%	1.9%	5.8%	3.2%	5.0%	1.8%	2.1%	1.5%	0.4%	0.4%	1.5%	1.7%	5.8%	0.5%	1.2%	
U	W	S	H	A	C	T	I		E	D	B	O	L	R	M	P	G	N	K	V	Y	N	J	F	

Text After Substitution:

```
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 ENTENDED FAMILY WERE ORIGINALLY USED TO ENPLAIN 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 SENIST 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 ENCHANGE, AND A LENS THROUGH WHICH TO VIEW
BROADER DIGITAL CULTURE. *.DUPONT AND A.CATTAPAN CRYPTOCOUPLE
```

3.2.



STEFA NIACA RUTAS U = RDGBL GAUJM WCMUY M