Cryptology: Classical Ciphers and their Cryptanalysis

Nilanjan Datta

Institute for Advancing Intelligence, TCG Crest

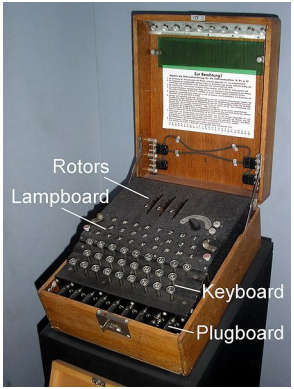
tcg crest

Inventing Harmonious Future

Historic Ciphers: Scytale

Historic Ciphers: Enigma Machine

https://www.youtube.com/watch?v=ybkkiGtJmkM



Classical Ciphers

- Shift Cipher
- Substitution Cipher
- Affine Cipher
- Vigenere Cipher
- Hill Cipher
- Permutation Cipher

Cryptanalysis of Shift Cipher

Cryptanalysis of Shift Cipher

Can you decipher the following text?

JBCRCLQRWCRVNBJENBWRWN,

Cryptanalysis of Shift Cipher

Can you decipher the following text?

JBCRCLQRWCRVNBJENBWRWN,

After applying brute force search:

jbcrclqrwcrvnbjenbwrwn
iabqbkpqvbqumaidmavqvm
hzapajopuaptlzhclzupul
gyzozinotzoskygbkytotk
fxynyhmnsynrjxfajxsnsj
ewxmxglmrxmqiweziwrmri
dvwlwfklqwlphvdyhvqlqh
cuvkvejkpvkogucxgupkpg
btujudijoujnftbwftojof
astitchintimesavesnine

Cryptanalysis of Affine Cipher

Cryptanalysis of Affine Cipher

Can you decipher the following text?

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH
```

Use frequency of characters.

Frequency Table of the English Language

letter	probability	letter	probability
A	.082	N	.067
B	.015	O	.075
C	.028	P	.019
D	.043	Q	.001
E	.127	R	.060
F	.022	S	.063
G	.020	T	.091
H	.061	U	.028
I	.070	V	.010
J	.002	W	.023
K	.008	X	.001
L	.040	Y	.020
M	.024	Z	.001

Cryptanalysis of Affine Cipher: Frequency Table for the Ciphertext

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH
```

letter	frequency	letter	frequency
A	2	N	1
B	1	O	1
C	0	P	2
D	7	Q	0
E	5	R	8
F	4	S	3
G	0	T	0
H	5	U	2
I	0	V	4
J	0	W	0
K	5	X	2
L	2	Y	1
M	2	Z	0

Cryptanalysis of Affine Cipher

Can you decipher the following text?

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH
```

- Guess: $e_K(e) = R,\ e_K(t) = D$

Cryptanalysis of Affine Cipher

Can you decipher the following text?

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH
```

- Guess: $e_K(e) = R,\ e_K(t) = D$
- Solve for $4a + b = 17,\ 19a + b = 3$.

Cryptanalysis of Affine Cipher

Can you decipher the following text?

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH
```

- Guess: $e_K(e) = R,\ e_K(t) = D$
- Solve for $4a + b = 17,\ 19a + b = 3$.
- Unique solution $a = 6,\ b = 19$. (Not Valid..!!)

Cryptanalysis of Affine Cipher

Can you decipher the following text?

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH
```

- Guess: $e_K(e) = R,\ e_K(t) = D$
- Solve for $4a + b = 17,\ 19a + b = 3$.
- Unique solution $a = 6,\ b = 19$. (Not Valid..!!)
- Guess: $e_K(e) = R,\ e_K(t) = H$

Cryptanalysis of Affine Cipher

Can you decipher the following text?

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH
```

- Guess: $e_K(e) = R,\ e_K(t) = D$
- Solve for $4a + b = 17,\ 19a + b = 3$.
- Unique solution $a = 6,\ b = 19$. (Not Valid..!!)
- Guess: $e_K(e) = R,\ e_K(t) = H$
- Solution $a = 3,\ b = 5$

Cryptanalysis of Affine Cipher

Can you decipher the following text?

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH
```

Cryptanalysis of Affine Cipher

Can you decipher the following text?

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK
APRKDLYEVLRHHRH
```

Solving with $a = 3$, $b = 5$:

```
algorithmsarequitegeneraldefinitionsofarit
hmeticprocesses
```

Cryptanalysis of Substitution Cipher

Cryptanalysis of Substitution Cipher

Can you decipher the following text?

```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Cryptanalysis of Substitution Cipher: Frequency Table

letter	probability	letter	probability
A	.082	*N*	.067
B	.015	*O*	.075
C	.028	*P*	.019
D	.043	*Q*	.001
E	.127	*R*	.060
F	.022	*S*	.063
G	.020	*T*	.091
H	.061	*U*	.028
I	.070	*V*	.010
J	.002	*W*	.023
K	.008	*X*	.001
L	.040	*Y*	.020
M	.024	*Z*	.001

Cryptanalysis of Substitution Cipher: Frequency Table

Look at di-grams:

$$TH, HE, IN, ER, AN, RE, ED, ON, ES, ST,$$
$$EN, AT, TO, NT, HA, ND, OU, EA, NG, AS,$$
$$OR, TI, IS, ET, IT, AR, TE, SE, HI, OF.$$

Cryptanalysis of Substitution Cipher: Frequency Table

Look at di-grams:

$$TH, HE, IN, ER, AN, RE, ED, ON, ES, ST,$$
$$EN, AT, TO, NT, HA, ND, OU, EA, NG, AS,$$
$$OR, TI, IS, ET, IT, AR, TE, SE, HI, OF.$$

Also look at tri-grams:

$$THE, ING, AND, HER, ERE, ENT,$$
$$THA, NTH, WAS, ETH, FOR, DTH.$$

Cryptanalysis of Substitution Cipher: Frequency of Occurances

```
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Cryptanalysis of Substitution Cipher: Frequency Table

letter	frequency	letter	frequency
A	0	N	9
B	1	O	0
C	15	P	1
D	13	Q	4
E	7	R	10
F	11	S	3
G	1	T	2
H	4	U	5
I	5	V	5
J	11	W	8
K	1	X	6
L	0	Y	10
M	16	Z	20

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.
- Look at digrams of the form $\_Z$ and $Z\_$.

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.
- Look at digrams of the form $\_Z$ and $Z\_$.
- $ZW : 4$, $WZ : 0$, W less frequent: $d_K(W) = d$

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.
- Look at digrams of the form $\_Z$ and $Z\_$.
- $ZW : 4$, $WZ : 0$, W less frequent: $d_K(W) = d$
- $DZ : 4$, $ZD : 2$: $d_K(D) \in \{r, s, t\}$

Cryptanalysis of Substitution Cipher

- Z occurs 20 times: $d_K(Z) = e$
- C, D, F, J, M, R, Y might be encryptions of t, a, o, i, n, s, h, r, but difficult to predict.
- Look at digrams of the form $\_Z$ and $Z\_$.
- $ZW : 4$, $WZ : 0$, W less frequent: $d_K(W) = d$
- $DZ : 4$, $ZD : 2$: $d_K(D) \in \{r, s, t\}$
- $ZRW : 1$, $RW : 2$, R frequent: $d_K(R) = n$

Cryptanalysis of Substitution Cipher

```
------end---------e----ned---e-----------
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ

--------e----e---------n--d---en----e----e
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ

-e---n------n------ed---e---e--ne-nd-e-e--
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ

-ed-----n-----------e----ed-------d---e--n
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Cryptanalysis of Substitution Cipher

```
------end-----a---e-a--nedh--e------a-----
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ

h-------ea---e-a---a---nhad-a-en--a-e-h--e
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ

he-a-n------n------ed---e---e--neandhe-e--
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ

-ed-a---nh---ha---a-e----ed-----a-d--he--n
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Cryptanalysis of Substitution Cipher

```
o-r-riend-ro--arise-a-inedhise--t---ass-it
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ

hs-r-riseasi-e-a-orationhadta-en--ace-hi-e
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ

he-asnt-oo-in-i-o-redso-e-ore-ineandhesett
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ

-ed-ac-inhischair-aceti-ted--to-ardsthes-n
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR
```

Cryptanalysis of Substitution Cipher

Our friend from Paris examined his empty glass with surprise, as if evaporation had taken place while he wasn't looking. I poured some more wine and he settled back in his chair, face tilted up towards the sun.[1]

Cryptanalysis of Vigenere Cipher

Cryptanalysis of Vigenere Cipher

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE

Cryptanalysis of Vigenere Cipher

- How can you find m?
- Given m, how can you decrypt?

Cryptanalysis of Vigenere Cipher

- How can you find m?
- Given m, how can you decrypt?

Can you use the following result?

- Index of coincidence: $I_c(\mathrm{x})$ denotes the probability that two random elements of $\mathrm{x} = (x_1 x_2 \cdots x_n)$ are identical.
- For a set of 26 random elements, $I_c(\mathrm{x}) = \frac{1}{26} = 0.038$
- However, for english dictionary $I_c(\mathrm{x}) = 0.065$