SANKET SANJAYPANT HIRE (2016CS50402)

Tutorial 2

Question 1- PlayFair Cipher

Cipher Text to decipher-

EGHXBYDPAIIKEHXCBXBOICPBKCDPBSOZTPFSQTCUOWEGCHMQLOGCQCPQABDCUL
BEPHZXDPTSCEXTTPEGHXOFWGCUIAPDPHLUBMUEPHULZRXGHOHDPLXGQIPEDNUS
PUEZCLBWIKOEPHDHEHXUMBFSAKYGEBCXHEYBDAELMSZRSDGQAEEIBOCECGWNC
BDQBYWGPHUHHUDEPHYBTMULOBHVKMBQICALDMCUETNLBMLMACRTIKEPUSUEIKO
ELAXACPLEIUPTPUXDPMUKOCUXHSQSDXTPDBUDNOUECUESIFQBOSTHELMUSEWDN
OUECUECILOQAOLZKSFOKBOUBDRES

Deciphered Text-

THE POWER OF HIS EYES WAS CONSIDERABLY ENHANCED BY THEIR POSITION PLACED AS THEY WERE BETWEEN THE PAINTED FOREHEAD AND THE DARK WHISKERS WHICH STREAMED X DOWN HIS CHEEKS EVEN A HALF WITS EYES WOULD SPARKLE IN SUCH A SETTING TO CROWN THE EFFECT HE WOUND A SAFXFRON COLOURED TURBAN AROUND HIS HEAD THIS COLOUR SCHEME NEVER FAILED PEOPLE WERE ATTRACTED TO HIM AS BEES ARE ATXTRACTED TO COSMOS OR DAHLIA STALKS X

Cleaning it further we get deciphered text as -

THE POWER OF HIS EYES WAS CONSIDERABLY ENHANCED BY THEIR POSITION PLACED AS THEY WERE BETWEEN THE PAINTED FOREHEAD AND THE DARK WHISKERS WHICH STREAMED DOWN HIS CHEEKS EVEN A HALF WITS EYES WOULD SPARKLE IN SUCH A SETTING TO CROWN THE EFFECT. HE WOUND A SAFFRON COLOURED TURBAN AROUND HIS HEAD. THIS COLOUR SCHEME NEVER FAILED. PEOPLE WERE ATTRACTED TO HIM AS BEES ARE ATTRACTED TO COSMOS OR DAHLIA STALKS.

The algorithm used for breaking PlayFair Cipher: Simulated Annealing

Approach:

Simulated Annealing is useful to get required permutation of key(global optima) in the presence of a large number of other permutations of key(local optima).

Since the PlayFair key is a (5 x 5) matrix, therefore, the key will contain 25 unique letters from A-Z.

Pseudocode:

```
Generate a 25 letter random key (let's call it parent key)
Decrypt the PlayFair Cipher Text using parent key
Calculate the fitness of the parent key  as a logarithm of the probability of the parent key
For temp = 10  to 0, temp = temp - step
        For transitions = 50000 to 0, transitions = transitions - 1
                Set child = shuffle(parent key) // swap two letters in parent key randomly
                Calculate the fitness of the child key as a logarithm of the probability of the child key
                Let delta_fitness = fitness of the child key - fitness of the parent key
                If (delta_fitness > 0) then { parent key = child key }
                Else if (delta_fitness < 0) then { parent key = child key with probability e^(-delta_fitness/temp) }
```

Calculating Fitness:

Fitness of key is calculated by deciphering ciphertext with that key and applying n-gram (in this case - quadgram statistics) statistical test on deciphered text (i.e. computing similarity with English text quadgrams.)

If we get stuck in the algorithm we can use these techniques on key - swapping rows, swapping columns, reversing the key, flipping the key square left to right or top to bottom.

[Reference: Practical Cryptography]

Key used to decipher:

G H I K F
N P Q R M
W X Y Z V
B S O L A
T E C D U

Question 2- Simple Cipher

Cipher Text to decipher:
Nbzmnzi rh z xlfmgib rm Zhrz. Nzmb Ilsrmtbz Nfhornh orev gsviv. Gsvri orevh ziv evib wruurxfog. Gsvb nfhg nrtizgv z olg. Rm 2017, gsviv rh hgilmt nrorgzib zxgrlm ztzrmhg Ilsrmtbz Nfhornh. Gsviv rh z olg lu erlovmxv. Nzmb kvlkov wrv. Z olg lu kvlkov ifm zdzb gl zmlgsvi xlfmgib. Hlnv kvlkov yvorvev gszg gsviv rh tvmlxrwv lu gsv Ilsrmtbzh. Gsv Nbzmnzi tlevimnvmg zhph z xlnnrggvv gl urmw lfg dszg szkkvmh. Gsv xlnnrggvv hzbh gszg gsviv rh ml tvmlxrwv. Sldvevi, gsviv rh hvirlfh xirnv. Z olg lu kvlkov wl mlg yvorvev gsrh. Gsvb hzb gszg gsv tlevimnvmg dzmgh gl srwv gsv gifgs.

Deciphered Text:
Myanmar is a country in Asia. Many Rohingya Muslims live there. Their lives are very difficult. They must migrate a lot. In 2017, there is strong military action against Rohingya Muslims. There is a lot of violence. Many people die. A lot of people run away to another country. Some people believe that there is genocide of the Rohingyas. The Myanmar government asks a committee to find out what happens. The committee says that there is no genocide. However, there is serious crime. A lot of people do not believe this. They say that the government wants to hide the truth.

Key used to decipher:
Substitution as follows
Cipher letter : 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
Decipher letter : Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Such that (A -> Z), (B-> Y), and so on.

Approach:
Frequency analysis of monograms, digrams, etc in English text and substituting those partially deciphered letters in other words and iterate until we get a complete English plaintext.
E.g, In given ciphertext, z is a one-letter word from frequency analysis (z->a)

To get more idea of the approach, check the approach section of question 3.

Question 3- Simple Cipher

Cipher Text to decipher:
Htghst xlt lxflekttfl zg hkgztez zitok laof ykgd zit lxf. Zitkt ol q ftv lzxrn. Oz lqnl ziqz lgdt eitdoeqsl of lxflekttfl utz ofzg htghst'l wsggr Leotfzolzl ztlz ygxk royytktfz lxflekttfl qfr lob eitdoeqsl. Zitn yofr ziqz qss lob eitdoeqsl utz ofzg zit wgrn. Zitn rg fgz afgv viqz zitlt eitdoeqsl rg zg htghst. Oz ol vgkknofu. Leotfzolzl dxlz rg dgkt ktltqkei zg xfrtklzqfr igv eitdoeqsl utz ofzg zit wgrn.

Deciphered Text:
People use sunscreens to protect their skin from the sun. There is a new study. It says that some chemicals in sunscreens get into people's blood Scientists test four different sunscreens and six chemicals. They find that all six chemicals get into the body. They do not know what these chemicals do to people. It is worrying. Scientists must do more research to understand how chemicals get into the body.

Key used to decipher:
Substitution as follows:
Cipher letter : Q W E R T Y U I O P A S D F G H J K L Z X C V B N M
Decipher letter : 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

Such that (Q -> A), (W -> B), and so on.

Approach:
Frequency analysis of monograms, digrams, etc in English text and substituting those partially deciphered letters in other words and iterate until we get a complete English plaintext.
E.g, In given ciphertext, q is a one-letter word from frequency analysis (q->a)
Now do analysis on “Oz” :
From the analysis as its first word of the sentence it can either one of these:
“It”, “In”, “As”, ”To”, etc take these mappings with “Oz”
And do further analysis
Like, take “Oz” -> “It” .....(A)
Then “ol” is after “Oz”, that is “ol” is after “It”. From the analysis we get “ol” -> “is” ……....(B)
Similarly, “of” -> “in” ……(C)

From (A), (B) and (C),
“o” -> “i”, “z” -> “t”, “l” -> “s”, “f” -> “n”, and so on.
