Computational Complexity of Implementation of the following techniques.

1. Playfair Cipher

After splitting the plaintext into digraphs the playfair cipher uses binary format to process it. The time complexity for both the encryption and decryption is linear((O(n)), because constant time lookups and swaps are carried for every digraph in the 5x5 matrix. Creation of key square is a constant time operation that takes O(1) time because it is a 5x5 matrix with 25 characters. Thus the overall time complexity for the encryption and decryption is O(n) where n is the number of digraphs.

2. Hill Cipher

The encryption complexity is O(nm2), where m is the block size and the decryption complexity is O(m3+nm2). Every plaintext block needs to be multiplied by an O(m2) m×m key matrix for it to be encrypted. The total complexity is O(nm2), since we encrypt O(n/m) blocks. The decryption process (using Gaussian elimination or determinant methods) which has a has O(m3) complexity requires the computation of the inverse of the key matrix. Decryption has the same complexity as encryption O(nm2), once the inverse matrix is obtained.

3. Vigenère Cipher

It has a linear complexity for both the encryption and decryption process of O(n) where n is the length of the plaintext or ciphertext. Based on the repeating key in both the process, every character needs a constant-time operation. These operations are carried out for every letter separately. Then the key and the plaintext must be stored. Its space complexity is O(n). Thus this cipher design process is effective in terms of both space and time complexity.

Mathematical Explanation of breaking of each cipher using Cryptanalysis

Playfair Cipher

- Playfair substitution scheme is a digraph-to-digraph transformation and its single-letter frequency analysis is not possible. Still, the bigram frequency analysis is enough to break it. Mathematical Description: Let C be the ciphertext and P be the plaintext. Each digraph transformation obeys particular rules of Playfair given below either the same row/column or diagonal swap etc. We obtain frequent digraphs from a large text collection, for example, English texts such that "TH", "HE", and "IN" appear with maximum frequency. By comparing ciphertext digraph frequencies with known bigram frequencies, we reconstruct the 5×5 key matrix.

Steps to Break It:

Collect Ciphertext Digraphs → Identify repeated pairs.

Compare with Known Frequencies → Match them with common English digraphs.

Reconstruct the Key Matrix → Based on observed patterns and digraph transformations.

The frequency of a digraph is given by:

$P(D_i)$= Count/N

- $P(D_i)$ is the probability of Di
- Count(D_i) is the number of occurrences of D_i in the ciphertext.
- N is the total number of digraphs.

Example: If we observe the presence of "BM" frequently in ciphertext and anticipate that the "TH" will be a frequent sequence in plaintext, we hypothesize "BM" stands for "TH" and modify the key square accordingly.

2. Cryptanalysis of Hill Cipher

- The Hill cipher is an encryption of plaintext using matrix multiplication as follows. C = KPmod26

where C is the ciphertext vector, K is the encryption matrix, P is the plaintext vector.

Mathematical Breakdown:

Assume we have n plaintext-ciphertext pairs. We set up the following system of linear equations:

KP_1=C_1mod 26

KP_2=C_2mod 26 and so on.

Write in matrix form: C = KP mod 26

Solve for K, $K = CP^{-1}mod26$, where P^{-1} is the modular inverse of the plaintext matrix.

Conditions for Breaking:

• The inverse of P must exist.

• If enough plaintext-ciphertext pairs are available, solving for K becomes trivial using Gaussian elimination.

3. Cryptanalysis of Vigenère Cipher

A recurring keyword is used in the Vigenère cipher, which causes periodic shifts in the letters. If the key length k is short, patterns in letter frequencies become visible.

Index of Coincidence for Key Length Estimation:

$IC=\sum_{i=1}^{26} \frac{fi(fi-1)}{N(N-1)}$

Where,

• f_i is the frequency of letter I

• N is the total no.of letters.

Compare with English IC (0.068) vs. Random IC (0.038). If the key length is close to 0.038, it is long. If it is higher, there is likely a shorter repeating key.

Estimating the key length using the Friedman Test:

k = 0.027N/(0.065 - IC) + N(IC-0.038)

Where, N is the length of the ciphertext and IC is the computed index of coincidence.

- IC helps distinguish Vigenère cipher from monoalphabetic ciphers.
- It provides an initial estimate of key length, refined by Kasiski examination.
- Once key length is known, frequency analysis helps determine shifts, revealing the plaintext.

Description of Hybrid Cipher Design Process

Design Process:

First, plaintext is subjected to the Hill Cipher (Substitution). The Hill cipher is used to replace each of the three-letter blocks that make up the plaintext.

The ciphertext that was produced using the Hill cipher is then subjected to Columnar Transposition (Transposition). For additional scrambling, the Hill ciphertext is first divided into rows, and then the columns are rearranged according to a keyword.

In order to add additional security, the procedure combines the two methods. The transposition guarantees that patterns in the ciphertext are more obscured, while the substitution in the Hill cipher adds complexity.

2. Hybrid Cipher Encryption and Decryption Example

Step 1: Hill Cipher Encryption

Consider the plaintext "HELLO", and the key matrix for the Hill cipher as:

$$K=\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Plaintext: "HELLO"

The letters are converted to their corresponding numerical values based on the alphabet where A=0, B=1, ..., Z=25:

- H = 7, E = 4, L = 11, L = 11, O = 14.

We break the plaintext into a 3x1 vector and then multiply by the key matrix:

$$P=\begin{bmatrix} 7 \\ 4 \\ 11 \end{bmatrix}$$

Matrix multiplication gives us the encrypted values, and applying the modulo 26 operation gives the ciphertext.

Step 2: Encryption using Columnar Transposition

The columnar transposition method is then used to rearrange the ciphertext. A matrix structure consisting of rows and columns will be used to write the final Hill cipher ciphertext, and the keyword will dictate the order in which the columns are read.

For example, if the Hill cipher output is "RIJVSU" and the keyword is "SECRET", we would arrange the ciphertext in columns based on the keyword, then read the columns in order.

Procedure for Decryption

The decryption procedure is comprised of the next actions:

Columnar Transposition Decryption: Go down the steps, that is, transposing the column back to its original form, after which the result can be found from Hill cipher encryption

Hill Cipher Decryption: To decipher, use matrix which is the inverse of Hill Cipher Key.

Security Evaluation of the Hybrid Cipher

The mixture of substitution and transposition in the hybrid cipher (Hill cipher

and Columnar Transposition) is what makes it more secure than using these technologies separately. Like a hybrid lock, which is more difficult to manipulate with break-ins and ward-off thieves by sticking to one way.

1. Hill Cipher Strength

- Strength:
- The Hill cipher, when applied with a 3x3 matrix, generates an encryption strength comparable to 128 bits. Consequently, in the 3x3 matrix, there are 9 entries and each can take on 26 different values. Therefore, this matrix yields us the number of potential keys, that is the possible keys may range from approximately possible key combinations.
- Vulnerability: A single Hill cipher alone is still prone to known-plaintext attacks, which is one of the biggest threats to the ciphertext data today, a situation where the attacker can recover the key matrix from pairs of plaintext-ciphertext. This vulnerability is lessened by allying the Hill cipher with columnar transposition.

2. Columnar Transposition Strength

- Strength: By scrambling the patterns of the ciphertext code through columns, the transposition ciphers the data in an added layer of security. It causes the hackers difficulty in identifying the patterns or the frequency isolation even if it does not provide any encryption on its own.
- Vulnerability: The difficulty posed by anagrams can be averted if the key is longer or more complicated, this way, the breakers have little chance to reveal the code, notwithstanding, this condition is higher when the decoded message contains more complex and longer sentences as well.

3. Combined Strength

The Combination:

The Hill cipher accompanying with columnar transposition allows a unique message to be hidden and secure even though only the receiver has the key which is used to decode the Hill cipher. It includes the overall security perception.

Brute-Force

Resistance: The use of the Hill cipher makes cracking the cipher through brute-force attacks almost impractical. Besides, the transposition is a preventive measure that makes it even more frequent for the hackers to guess the correct plaintext structure. In case, though, they could get some data, they cannot predict it at all.

4. Overall Security

Hybrid cipher is set out with a minimum of 128 encryption safety bits

. Indeed, the aforesaid concomitant utilization of both substitution and transposition strategies is the only steadfast warrant of the level of security above the standalone ciphering techniques.

Conclusion

The hybrid-based encrypting five-step algorithm, including the Hill cipher and columnar transposition, is highly effective. It increases the security of the coded information by introducing both substitution and transposition IMPs that makes it more coercible as a duo when contrasted with just one of them. The Hill cipher is a strong type of encryption with a 3x3 matrix, whilst the transposition would ensure the ciphertext is less prone to pattern analysis. Specified marketing arrangements such as encryption keys of minimum 128-bit strength are its main feature, hence it is highly secure for communication.

Computational Complexity of Implementation

by Nidhi N Pai .

Submission date: 12-Feb-2025 03:41PM (UTC+0530)
Submission ID: 2586543375
File name: Complexity_of_Implementation_of_the_following_techniques_1.docx (22.09K)
Word count: 1548
Character count: 8268

Computational Complexity of Implementation of the following techniques.

1. Playfair Cipher

After splitting the plaintext into digraphs the playfair cipher uses binary format to process it. The time complexity for both the encryption and decryption is linear((O(n)), because constant time lookups and swaps are carried for every digraph in the 5x5 matrix. Creation of key square is a constant time operation that takes O(1) time because it is a 5x5 matrix with 25 characters. Thus the overall time complexity for the encryption and decryption is O(n) where n is the number of digraphs.

2. Hill Cipher

The encryption complexity is O(nm2), where m is the block size and the decryption complexity is O(m3+nm2). Every plaintext block needs to be multiplied by an O(m2) m×m key matrix for it to be encrypted. The total complexity is O(nm2), since we encrypt O(n/m) blocks. The decryption process (using Gaussian elimination or determinant methods) which has a has O(m3) complexity requires the computation of the inverse of the key matrix. Decryption has the same complexity as encryption O(nm2), once the inverse matrix is obtained.

3. Vigenère Cipher

It has a linear complexity for both the encryption and decryption process of O(n) where n is the length of the plaintext or ciphertext. Based on the repeating key in both the process, every character needs a constant-time operation. These operations are carried out for every letter separately. Then the key and the plaintext must be stored. Its space complexity is O(n). Thus this cipher design process is effective in terms of both space and time complexity.

Mathematical Explanation of breaking of each cipher using Cryptanalysis

Playfair Cipher

- Playfair substitution scheme is a digraph-to-digraph transformation and its single-letter frequency analysis is not possible. Still, the bigram frequency analysis is enough to break it. Mathematical Description: Let C be the ciphertext and P be the plaintext. Each digraph transformation obeys particular rules of Playfair given below either the same row/column or diagonal swap etc. We obtain frequent digraphs from a large text collection, for example, English texts such that "TH", "HE", and "IN" appear with maximum frequency. By comparing ciphertext digraph frequencies with known bigram frequencies, we reconstruct the 5×5 key matrix.

Steps to Break It:

Collect Ciphertext Digraphs → Identify repeated pairs.

Compare with Known Frequencies → Match them with common English digraphs.

Reconstruct the Key Matrix → Based on observed patterns and digraph transformations.

The frequency of a digraph is given by:

$P(D_i)$= Count/N

- $P(D_i)$ is the probability of Di
- Count(D_i) is the number of occurrences of D_i in the ciphertext.
- N is the total number of digraphs.

Example: If we observe the presence of "BM" frequently in ciphertext and anticipate that the "TH" will be a frequent sequence in plaintext, we hypothesize "BM" stands for "TH" and modify the key square accordingly.

2. Cryptanalysis of Hill Cipher

- The Hill cipher is an encryption of plaintext using matrix multiplication as follows. C = KPmod26

where C is the ciphertext vector, K is the encryption matrix, P is the plaintext vector.

Mathematical Breakdown:

Assume we have n plaintext-ciphertext pairs. We set up the following system of linear equations:

KP_1=C_1 mod 26

KP_2=C_2 mod 26 and so on.

Write in matrix form: C = KP mod 26

Solve for K, $K = CP^{-1} mod 26$, where P^{-1} is the modular inverse of the plaintext matrix.

Conditions for Breaking:

• The inverse of P must exist.

• If enough plaintext-ciphertext pairs are available, solving for K becomes trivial using Gaussian elimination.

3. Cryptanalysis of Vigenère Cipher

A recurring keyword is used in the Vigenère cipher, which causes periodic shifts in the letters. If the key length k is short, patterns in letter frequencies become visible.

Index of Coincidence for Key Length Estimation:

$IC=\sum_{i=1}^{26} \frac{fi(fi-1)}{N(N-1)}$

Where,

• f_i is the frequency of letter I

• N is the total no.of letters.

Compare with English IC (0.068) vs. Random IC (0.038). If the key length is close to 0.038, it is long. If it is higher, there is likely a shorter repeating key.

Estimating the key length using the Friedman Test:

$k = 0.027N/((0.065 - IC) + N(IC-0.038)$

Where, N is the length of the ciphertext and IC is the computed index of coincidence.

- IC helps distinguish Vigenère cipher from monoalphabetic ciphers.
- It provides an initial estimate of key length, refined by Kasiski examination.
- Once key length is known, frequency analysis helps determine shifts, revealing the plaintext.

Description of Hybrid Cipher Design Process

Design Process:

First, plaintext is subjected to the Hill Cipher (Substitution). The Hill cipher is used to replace each of the three-letter blocks that make up the plaintext.

The ciphertext that was produced using the Hill cipher is then subjected to Columnar Transposition (Transposition). For additional scrambling, the Hill ciphertext is first divided into rows, and then the columns are rearranged according to a keyword.

In order to add additional security, the procedure combines the two methods. The transposition guarantees that patterns in the ciphertext are more obscured, while the substitution in the Hill cipher adds complexity.

2. Hybrid Cipher Encryption and Decryption Example

Step 1: Hill Cipher Encryption

Consider the plaintext "HELLO", and the key matrix for the Hill cipher as:

$$K=\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Plaintext: "HELLO"

The letters are converted to their corresponding numerical values based on the alphabet where A=0, B=1, ..., Z=25:

- H = 7, E = 4, L = 11, L = 11, O = 14.

We break the plaintext into a 3x1 vector and then multiply by the key matrix:

$$P=\begin{bmatrix} 7 \\ 4 \\ 11 \end{bmatrix}$$

Matrix multiplication gives us the encrypted values, and applying the modulo 26 operation gives the ciphertext.

Step 2: Encryption using Columnar Transposition

The columnar transposition method is then used to rearrange the ciphertext. A matrix structure consisting of rows and columns will be used to write the final Hill cipher ciphertext, and the keyword will dictate the order in which the columns are read.

For example, if the Hill cipher output is "RIJVSU" and the keyword is "SECRET", we would arrange the ciphertext in columns based on the keyword, then read the columns in order.

Procedure for Decryption

The decryption procedure is comprised of the next actions:

Columnar Transposition Decryption: Go down the steps, that is, transposing the column back to its original form, after which the result can be found from Hill cipher encryption

Hill Cipher Decryption: To decipher, use matrix which is the inverse of Hill Cipher Key.

Security Evaluation of the Hybrid Cipher

The mixture of substitution and transposition in the hybrid cipher (Hill cipher

and Columnar Transposition) is what makes it more secure than using these technologies separately. Like a hybrid lock, which is more difficult to manipulate with break-ins and ward-off thieves by sticking to one way.

1. Hill Cipher Strength

- Strength:
- The Hill cipher, when applied with a 3x3 matrix, generates an encryption strength comparable to 128 bits. Consequently, in the 3x3 matrix, there are 9 entries and each can take on 26 different values. Therefore, this matrix yields us the number of potential keys, that is the possible keys may range from approximately possible key combinations.
- Vulnerability: A single Hill cipher alone is still prone to known-plaintext attacks, which is one of the biggest threats to the ciphertext data today, a situation where the attacker can recover the key matrix from pairs of plaintext-ciphertext. This vulnerability is lessened by allying the Hill cipher with columnar transposition.

2. Columnar Transposition Strength

- Strength: By scrambling the patterns of the ciphertext code through columns, the transposition ciphers the data in an added layer of security. It causes the hackers difficulty in identifying the patterns or the frequency isolation even if it does not provide any encryption on its own.
- Vulnerability: The difficulty posed by anagrams can be averted if the key is longer or more complicated, this way, the breakers have little chance to reveal the code, notwithstanding, this condition is higher when the decoded message contains more complex and longer sentences as well.

3. Combined Strength

The Combination:

The Hill cipher accompanying with columnar transposition allows a unique message to be hidden and secure even though only the receiver has the key which is used to decode the Hill cipher. It includes the overall security perception.

Brute-Force

Resistance: The use of the Hill cipher makes cracking the cipher through brute-force attacks almost impractical. Besides, the transposition is a preventive measure that makes it even more frequent for the hackers to guess the correct plaintext structure. In case, though, they could get some data, they cannot predict it at all.

4. Overall Security

Hybrid cipher is set out with a minimum of 128 encryption safety bits

. Indeed, the aforesaid concomitant utilization of both substitution and transposition strategies is the only steadfast warrant of the level of security above the standalone ciphering techniques.

Conclusion

The hybrid-based encrypting five-step algorithm, including the Hill cipher and columnar transposition, is highly effective. It increases the security of the coded information by introducing both substitution and transposition IMPs that makes it more coercible as a duo when contrasted with just one of them. The Hill cipher is a strong type of encryption with a 3x3 matrix, whilst the transposition would ensure the ciphertext is less prone to pattern analysis. Specified marketing arrangements such as encryption keys of minimum 128-bit strength are its main feature, hence it is highly secure for communication.

Computational Complexity of Implementation

ORIGINALITY REPORT

5%	0%	1%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Prairie View A&M University Student Paper	2%
2	Submitted to De Montfort University Student Paper	1%
3	V. U. K. Sastry, S. Udaya Kumar, A. Vinaya babu. "A Large Block Cipher Using Modular Arithmetic Inverse of a Key Matrix and Mixing of the Key Matrix and the Plaintext", Journal of Computer Science, 2006 Publication	1%
4	Submitted to Sydney Institute of Technology and Commerce Student Paper	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		