CS3053 Computer Security
Historical Ciphers

Eng Prof Chandana Gamage
BSc Eng Hons, MEng, PhD, CEng
Department of Computer Science & Engineering
University of Moratuwa

July 24, 2023

Acknowledgment

These lecture notes are based on the *Chapter 7 on Historical Ciphers* of the textbook **Cryptography Made Simple**, by Nigel P Smart, Springer, 2016.

Introduction

An encryption algorithm (e), also called a *cipher*, transforms a plaintext (m) into a ciphertext (c) under the control of a secret key (k).

Introduction

An encryption algorithm (e), also called a *cipher*, transforms a plaintext (m) into a ciphertext (c) under the control of a secret key (k).

- This process is called encryption or encipherment and denoted as $c = e_k(m)$.

Introduction

An encryption algorithm (e), also called a *cipher*, transforms a plaintext (m) into a ciphertext (c) under the control of a secret key (k).

- This process is called encryption or encipherment and denoted as $c = e_k(m)$.
- The reverse process is called decryption (d) or decipherment and denoted as $m = d_k(c)$.

Introduction

An encryption algorithm (e), also called a *cipher*, transforms a plaintext (m) into a ciphertext (c) under the control of a secret key (k).

- This process is called encryption or encipherment and denoted as $c = e_k(m)$.
- The reverse process is called decryption (d) or decipherment and denoted as $m = d_k(c)$.
- It is important to note that encryption and decryption algorithms (e and d) are public and we assume that ciphertext (c) can also be easily (that is, publicly) accessed.

Secret Key

The secrecy of plaintext (m) is totally dependent on the secrecy of the key (k).

Secret Key

The secrecy of plaintext (m) is totally dependent on the secrecy of the key (k).

- This scheme requires both parties to a secret communication to know the key (k) and keep it secret.

Secret Key

The secrecy of plaintext (m) is totally dependent on the secrecy of the key (k).

- This scheme requires both parties to a secret communication to know the key (k) and keep it secret.
- Algorithms with this property are called *symmetric cryptosystems* or *secret key cryptosystems*.

Ciphers for Human Readable Languages

The ciphers used in the pre-computer era are called historical ciphers or classical ciphers.

Ciphers for Human Readable Languages

The ciphers used in the pre-computer era are called historical ciphers or classical ciphers.

- The historical ciphers used plaintext that was *human-readable* and was linked to
  - a particular language,
  - the alphabet of symbols or characters used, and
  - the peculiar statistical characteristics of the language.

Ciphers for Human Readable Languages

The ciphers used in the pre-computer era are called historical ciphers or classical ciphers.

- The historical ciphers used plaintext that was *human-readable* and was linked to
  - a particular language,
  - the alphabet of symbols or characters used, and
  - the peculiar statistical characteristics of the language.

- For example, the English language
- with 26 character alphabet (`A` to `Z`) and
- laguage-specific statistical characteristics
  - higher usage of characters `e`, `t`, `a`, `o`, `i` and
  - higher appearance of bigrams such as `th`, `he`, `an`, `in` or trigrams such as `the`, `ing`, `and`, `her`, `ere`.

Shift Cipher

In one of the earliest ciphers, the encryption was done by replacing each letter in the alphabet by a letter located at a specific fixed distance from that letter.

Shift Cipher

In one of the earliest ciphers, the encryption was done by replacing each letter in the alphabet by a letter located at a specific fixed distance from that letter.

- For example, if the fixed distance value is 3, then the letter `A` would be replaced by letter `D` and the plaintext word `HELLO` would be encrypted as ciphertext `KHOOR`.

Shift Cipher

In one of the earliest ciphers, the encryption was done by replacing each letter in the alphabet by a letter located at a specific fixed distance from that letter.

- For example, if the fixed distance value is 3, then the letter `A` would be replaced by letter `D` and the plaintext word `HELLO` would be encrypted as ciphertext `KHOOR`.
- This value by which the alphabet is shifted is the secret key of the encryption scheme.

Shift Cipher

In one of the earliest ciphers, the encryption was done by replacing each letter in the alphabet by a letter located at a specific fixed distance from that letter.

- For example, if the fixed distance value is 3, then the letter `A` would be replaced by letter `D` and the plaintext word `HELLO` would be encrypted as ciphertext `KHOOR`.
- This value by which the alphabet is shifted is the secret key of the encryption scheme.
- When the key value is **3**, it is commonly called the *Caesar cipher*.

Shift Cipher as a Stream Cipher

The shift cipher for English language is generally denoted as $c = m + k \mod 25$ where we denote the letters of the plaintext alphabet m as integer values 0 (for a) to 25 (for z).

Shift Cipher as a Stream Cipher

The shift cipher for English language is generally denoted as $c = m + k \mod 25$ where we denote the letters of the plaintext alphabet m as integer values 0 (for a) to 25 (for z).

- We can consider this method of encryption as a *stream cipher* where a stream of plaintext characters (m_i) and a stream of keys (k_i) are input to a function $(m_i + k_i \mod 25)$ that output a stream of ciphertext characters (c_i).

Shift Cipher as a Stream Cipher

The shift cipher for English language is generally denoted as $c = m + k \bmod 25$ where we denote the letters of the plaintext alphabet m as integer values 0 (for a) to 25 (for z).

- We can consider this method of encryption as a *stream cipher* where a stream of plaintext characters (m_i) and a stream of keys (k_i) are input to a function $(m_i + k_i \bmod 25)$ that output a stream of ciphertext characters (c_i).
- In this shift cipher, the keystream has a repeating sequence of just one key value k.

Breaking the Shift Cipher

This cipher is quite easy to break as there are only 26 possible keys and an attacker can try each key in turn until the correct key is found.

Breaking the Shift Cipher

This cipher is quite easy to break as there are only 26 possible keys and an attacker can try each key in turn until the correct key is found.

- This is called an *exhaustive key search* attack.

Breaking the Shift Cipher

This cipher is quite easy to break as there are only 26 possible keys and an attacker can try each key in turn until the correct key is found.

- This is called an *exhaustive key search* attack.
- For this attack to be successful, the attacker must be able to *recognize* the correct plaintext when the key used originally for encryption is tried.

Breaking Ciphers by Statistical Techniques

Another technique to break this cipher is to use a statistical technique called *character frequency analysis*.

Breaking Ciphers by Statistical Techniques

Another technique to break this cipher is to use a statistical technique called *character frequency analysis*.

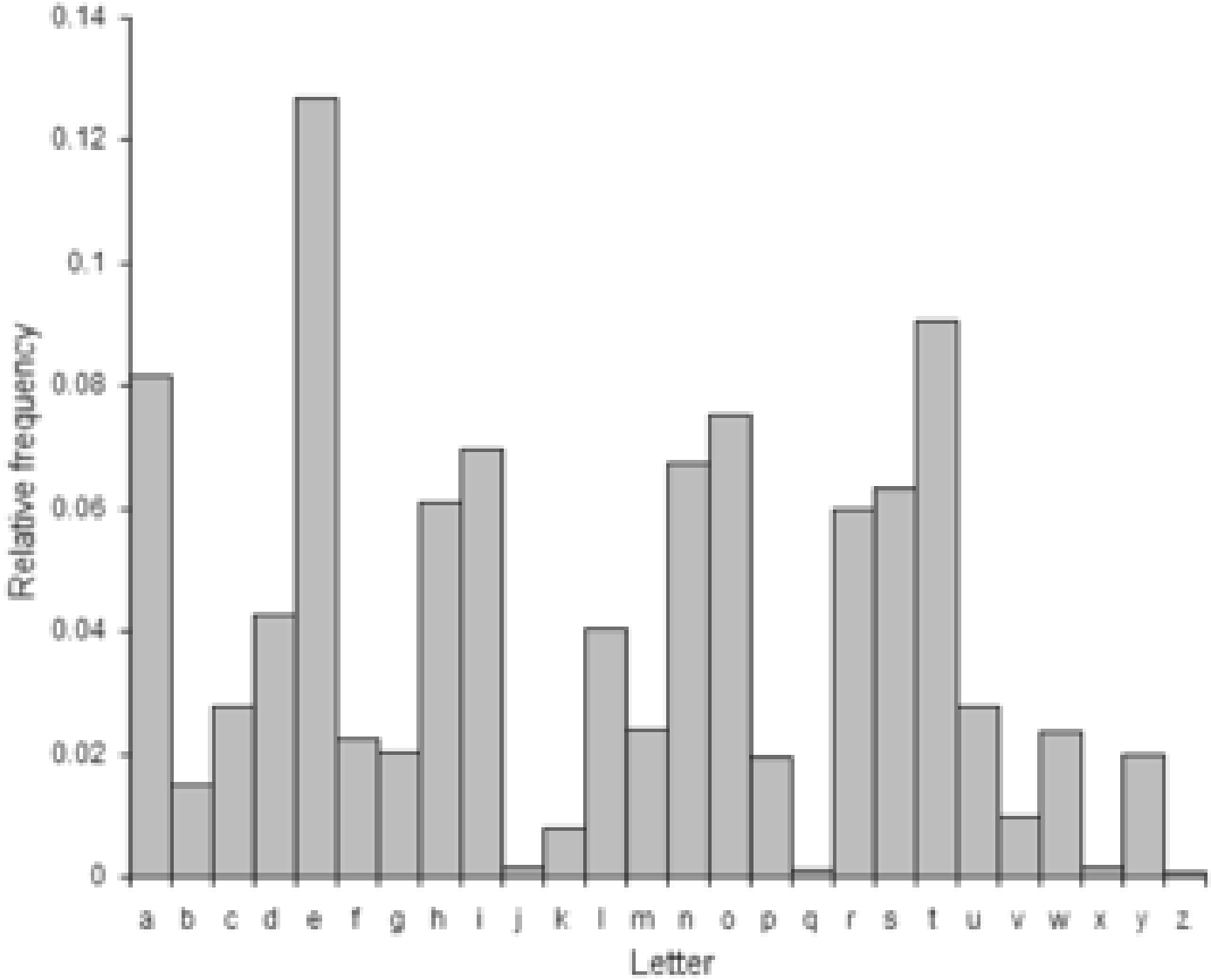
- This method will compute the frequency values for the characters in the ciphertext and match that with the character frequency table of the specific language (for example, English language).

Breaking Ciphers by Statistical Techniques

Another technique to break this cipher is to use a statistical technique called *character frequency analysis*.

- This method will compute the frequency values for the characters in the ciphertext and match that with the character frequency table of the specific language (for example, English language).
- We can take the characters with the highest frequencies in the ciphertext and replace them with corresponding plaintext characters according to the standard character frequency table.

Single Letter Frequency for English Language



Trial & Error for Statistical Analysis Attacks

What heuristics can we use in statistical cryptanalysis?

Trial & Error for Statistical Analysis Attacks

What heuristics can we use in statistical cryptanalysis?

- In character frequency analysis technique, we may have to experiment with different ordering of characters to find the correct key value.

Trial & Error for Statistical Analysis Attacks

What heuristics can we use in statistical cryptanalysis?

- In character frequency analysis technique, we may have to experiment with different ordering of characters to find the correct key value.
- However, as the 6 most frequently occurring characters account for approximately 44.4% of the characters in a block of text, the correct key value can be found easily.

Trial & Error for Statistical Analysis Attacks

What heuristics can we use in statistical cryptanalysis?

- In character frequency analysis technique, we may have to experiment with different ordering of characters to find the correct key value.
- However, as the 6 most frequently occurring characters account for approximately 44.4% of the characters in a block of text, the correct key value can be found easily.
- When you get just few ciphertext characters replaced with the correct plaintext characters, the original text becomes somewhat apparent even without a full decryption.

Statistical Distance in Shift Cipher Attacks 1/3

What measurements can we use in statistical cryptanalysis?

Statistical Distance in Shift Cipher Attacks 1/3

What measurements can we use in statistical cryptanalysis?

- Another way to find the correct key is to compute the *statistical distance* between the standard character frequency distribution (say, X) and the character frequency distribution computed from the ciphertext (say, Y).

Statistical Distance in Shift Cipher Attacks 2/3

As we can consider distribution Y to be representing 26 possible arrangements of the alphabet based on the possible values of k, we in fact have a set of distributions $Y_k : k = 0 \ldots 25$.

Statistical Distance in Shift Cipher Attacks 2/3

As we can consider distribution Y to be representing 26 possible arrangements of the alphabet based on the possible values of k, we in fact have a set of distributions $Y_k : k = 0 \ldots 25$.

- Thereafter, we can calculate a set of statistical distance values as

$$\Delta[X, Y_k] = \frac{1}{2} \sum_{u \in V} \left| \underset{X \leftarrow D_{standard}}{Pr} [X = u] - \underset{Y \leftarrow D_k}{Pr} [Y = u] \right|$$

- X: random variable distributed according to standard character frequency
- Y_k: random variables distributed according to particular k shift
- V: the set of values which can occur for X or Y with non-zero probability

Statistical Distance in Shift Cipher Attacks 3/3

From the 26 values of $\Delta(XY_k)$, we can find the smallest such value and take the corresponding k value as the secret key.

Substitution Cipher

The main weakness of shift ciphers is the small size of the key space allowing an attacker to easily carry out an exhaustive key search.

Substitution Cipher

The main weakness of shift ciphers is the small size of the key space allowing an attacker to easily carry out an exhaustive key search.

- In a substitution cipher, the key is created by a proper permutation of the plaintext alphabet rather than a simple shift of the alphabet.

Substitution Cipher

The main weakness of shift ciphers is the small size of the key space allowing an attacker to easily carry out an exhaustive key search.

- In a substitution cipher, the key is created by a proper permutation of the plaintext alphabet rather than a simple shift of the alphabet.
- This leads to the requirement that the key is now 26 different values corresponding to new positions of characters in standard alphabet rather than a single value as in shift ciphers.

Substitution Cipher

The main weakness of shift ciphers is the small size of the key space allowing an attacker to easily carry out an exhaustive key search.

- In a substitution cipher, the key is created by a proper permutation of the plaintext alphabet rather than a simple shift of the alphabet.
- This leads to the requirement that the key is now 26 different values corresponding to new positions of characters in standard alphabet rather than a single value as in shift ciphers.
- As the number of possible keys is equal to the number of permutations, an English language cipher could now have a key space of $26! \approx 4.03 \cdot 10^{26} \approx 2^{88}$.

Substitution Cipher

The main weakness of shift ciphers is the small size of the key space allowing an attacker to easily carry out an exhaustive key search.

- In a substitution cipher, the key is created by a proper permutation of the plaintext alphabet rather than a simple shift of the alphabet.
- This leads to the requirement that the key is now 26 different values corresponding to new positions of characters in standard alphabet rather than a single value as in shift ciphers.
- As the number of possible keys is equal to the number of permutations, an English language cipher could now have a key space of $26! \approx 4.03 \cdot 10^{26} \approx 2^{88}$.
- While this massive key space appears to make a substitution cipher unbreakable, these ciphers can still be attacked using statistical techniques based on language characteristics.

Poly-alphabetic Ciphers

How to thwart cryptanalysts using language characteristic statistics?

Poly-alphabetic Ciphers

How to thwart cryptanalysts using language characteristic statistics?

- A major weakness in both the shift cipher and the substitution cipher is that each plaintext character is always replaced by the same ciphertext character for the entire block of plaintext.

Poly-alphabetic Ciphers

How to thwart cryptanalysts using language characteristic statistics?

- A major weakness in both the shift cipher and the substitution cipher is that each plaintext character is always replaced by the same ciphertext character for the entire block of plaintext.
- This preserves the language characteristics of the plaintext in the ciphertext, leading to statistical analysis techniques for successful attacks on the ciphers.

Poly-alphabetic Ciphers

How to thwart cryptanalysts using language characteristic statistics?

- A major weakness in both the shift cipher and the substitution cipher is that each plaintext character is always replaced by the same ciphertext character for the entire block of plaintext.
- This preserves the language characteristics of the plaintext in the ciphertext, leading to statistical analysis techniques for successful attacks on the ciphers.
- A solution to this problem is to move from the *mono-alphabetic substitution ciphers* that uses a single substitution alphabet to *poly-alphabetic substitution ciphers* that use multiple substitution ciphers.

Poly-alphabetic Ciphers

How to thwart cryptanalysts using language characteristic statistics?

- A major weakness in both the shift cipher and the substitution cipher is that each plaintext character is always replaced by the same ciphertext character for the entire block of plaintext.
- This preserves the language characteristics of the plaintext in the ciphertext, leading to statistical analysis techniques for successful attacks on the ciphers.
- A solution to this problem is to move from the *mono-alphabetic substitution ciphers* that uses a single substitution alphabet to *poly-alphabetic substitution ciphers* that use multiple substitution ciphers.
- For example, we can use one substitution alphabet for all the characters in odd-numbered positions in a block of text and a different cipher for characters in even-numbered positions.

Improved Security in Poly-alphabetic Ciphers

The poly-alphabetic ciphers result in the same plaintext character in odd and even numbered positions in a block of texts being substituted by two different characters.

Improved Security in Poly-alphabetic Ciphers

The poly-alphabetic ciphers result in the same plaintext character in odd and even numbered positions in a block of texts being substituted by two different characters.

- This leads to changes in the character frequency graph leading it to become **flatter** and making it harder to identify the characters with a higher frequency of appearance in the text.

Improved Security in Poly-alphabetic Ciphers

The poly-alphabetic ciphers result in the same plaintext character in odd and even numbered positions in a block of texts being substituted by two different characters.

- This leads to changes in the character frequency graph leading it to become **flatter** and making it harder to identify the characters with a higher frequency of appearance in the text.
- The number of alphabets used in a poly-alphabetic substitution cipher can be increased to make it harder for attackers to break a cipher.

Improved Security in Poly-alphabetic Ciphers

The poly-alphabetic ciphers result in the same plaintext character in odd and even numbered positions in a block of texts being substituted by two different characters.

- This leads to changes in the character frequency graph leading it to become **flatter** and making it harder to identify the characters with a higher frequency of appearance in the text.
- The number of alphabets used in a poly-alphabetic substitution cipher can be increased to make it harder for attackers to break a cipher.
- For example, use of 5 alphabets would result in a total key space of $(26!)^5 \approx 2^{441}$. This massive key space is obtained at a relatively modest cost of having to remember a key of length $26 \cdot 5 = 130$ characters.

The Vigenère Cipher

This cipher was invented in 1533 by the Italian cryptologist Giovan Battista Bellaso.

The Vigenère Cipher

This cipher was invented in 1533 by the Italian cryptologist Giovan Battista Bellaso.

- It is named after the French French diplomat and cryptographer Blaise de Vigenère (1523-1596) due to a mis-attribution.

The Vigenère Cipher

This cipher was invented in 1533 by the Italian cryptologist Giovan Battista Bellaso.

- It is named after the French French diplomat and cryptographer Blaise de Vigenère (1523-1596) due to a mis-attribution.
- The cipher created by Vigenère is called *autokey cipher* and provides a higher level of security against attempts to break it.

The Vigenère Cipher

This cipher was invented in 1533 by the Italian cryptologist Giovan Battista Bellaso.

- It is named after the French French diplomat and cryptographer Blaise de Vigenère (1523-1596) due to a mis-attribution.
- The cipher created by Vigenère is called *autokey cipher* and provides a higher level of security against attempts to break it.
- The Vigenère cipher of Bellaso is a variant on the poly-alphabetic cipher scheme where the ciphertext alphabets used were restricted to only cyclic shifts of the standard alphabet.

The Vigenère Cipher

This cipher was invented in 1533 by the Italian cryptologist Giovan Battista Bellaso.

- It is named after the French French diplomat and cryptographer Blaise de Vigenère (1523-1596) due to a mis-attribution.
- The cipher created by Vigenère is called *autokey cipher* and provides a higher level of security against attempts to break it.
- The Vigenère cipher of Bellaso is a variant on the poly-alphabetic cipher scheme where the ciphertext alphabets used were restricted to only cyclic shifts of the standard alphabet.
- In this scheme, a 5 alphabet Vigenère cipher would only have a total key space of $26^5 \approx 2^{23}$ but at a cost of just 5 numeric values as the key, which is far easier to remember.

Vigenère Cipher as a Stream Cipher

We can view the Vigenère cipher as a stream cipher where the characters in the plaintext stream are replaced by integer values corresponding to their position in the standard alphabet and the keystream is a repetition of the short secret key (with each character in the key replaced by its equivalent position value).

Vigenère Cipher as a Stream Cipher

We can view the Vigenère cipher as a stream cipher where the characters in the plaintext stream are replaced by integer values corresponding to their position in the standard alphabet and the keystream is a repetition of the short secret key (with each character in the key replaced by its equivalent position value).

- The output ciphertext stream is the modulo addition of the plaintext stream value with keystream value.

Vigenère Cipher as a Stream Cipher

We can view the Vigenère cipher as a stream cipher where the characters in the plaintext stream are replaced by integer values corresponding to their position in the standard alphabet and the keystream is a repetition of the short secret key (with each character in the key replaced by its equivalent position value).

- The output ciphertext stream is the modulo addition of the plaintext stream value with keystream value.
- As expected from a poly-alphabetic substitution cipher, the same character in the plaintext is substituted by multiple different character in the ciphertext based on the positional value of the plaintext character in the input block of text.

Vigenère Cipher as a Stream Cipher

We can view the Vigenère cipher as a stream cipher where the characters in the plaintext stream are replaced by integer values corresponding to their position in the standard alphabet and the keystream is a repetition of the short secret key (with each character in the key replaced by its equivalent position value).

- The output ciphertext stream is the modulo addition of the plaintext stream value with keystream value.
- As expected from a poly-alphabetic substitution cipher, the same character in the plaintext is substituted by multiple different character in the ciphertext based on the positional value of the plaintext character in the input block of text.
- This results in a character frequency graph that is largely devoid of any significant peaks helping to identify characters with high frequency of appearance in the plaintext.

Attacking Vigenère Cipher

The security strength of Vigenère cipher depends significantly on keeping the length of the key secret.

Attacking Vigenère Cipher

The security strength of Vigenère cipher depends significantly on keeping the length of the key secret.

- If the length of the key is found, then the cipher can be attacked in the same manner as attacking shift ciphers using statistical properties of the plaintext language for each block of ciphertext extracted from separate keyword positions.

Attacking Vigenère Cipher

The security strength of Vigenère cipher depends significantly on keeping the length of the key secret.

- If the length of the key is found, then the cipher can be attacked in the same manner as attacking shift ciphers using statistical properties of the plaintext language for each block of ciphertext extracted from separate keyword positions.
- For example, the repeating keyword `HELLO` would give us 5 ciphertext blocks for characters at positions 1 to 5 repeating for the full length of the ciphertext.

Attacking Vigenère Cipher

The security strength of Vigenère cipher depends significantly on keeping the length of the key secret.

- If the length of the key is found, then the cipher can be attacked in the same manner as attacking shift ciphers using statistical properties of the plaintext language for each block of ciphertext extracted from separate keyword positions.
- For example, the repeating keyword `HELLO` would give us 5 ciphertext blocks for characters at positions 1 to 5 repeating for the full length of the ciphertext.
- As repeated character strings that in the plaintext that align to same positions of the keyword would result in the same ciphertext string, the ciphertext can be analyzed to find such repeating short strings.

Attacking Vigenère Cipher

The security strength of Vigenère cipher depends significantly on keeping the length of the key secret.

- If the length of the key is found, then the cipher can be attacked in the same manner as attacking shift ciphers using statistical properties of the plaintext language for each block of ciphertext extracted from separate keyword positions.
- For example, the repeating keyword `HELLO` would give us 5 ciphertext blocks for characters at positions 1 to 5 repeating for the full length of the ciphertext.
- As repeated character strings that in the plaintext that align to same positions of the keyword would result in the same ciphertext string, the ciphertext can be analyzed to find such repeating short strings.
- This often happens with commonly occurring bigrams and trigrams of the language.

Kasiski Test

A technique for determining the keyword length called the *Kasiski test* was published by the German infantry officer and cryptographer Major Friedrich Wilhelm Kasiski (1805 - 1881).

Kasiski Test

A technique for determining the keyword length called the *Kasiski test* was published by the German infantry officer and cryptographer Major Friedrich Wilhelm Kasiski (1805 - 1881).

- Once a repeating character sequence is located, the distances between multiple occurrences of the character string is counted and the greatest common divisor for these distance values would be the length of the keyword (or a multiple of that).

Kasiski Test

A technique for determining the keyword length called the *Kasiski test* was published by the German infantry officer and cryptographer Major Friedrich Wilhelm Kasiski (1805 - 1881).

- Once a repeating character sequence is located, the distances between multiple occurrences of the character string is counted and the greatest common divisor for these distance values would be the length of the keyword (or a multiple of that).
- As an aside, it is claimed that Charles Babbage, the British mathematician called the *father of the computer* has known about this technique earlier than Kasiski.

Playfair Cipher 1/2

This substitution cipher invented by Sir Charles Wheatstone in 1854 was the first digram substitution cipher.

Playfair Cipher 1/2

This substitution cipher invented by Sir Charles Wheatstone in 1854 was the first digram substitution cipher.

- It is named after Lord Playfair who promoted its use in diplomatic communication.

Playfair Cipher 1/2

This substitution cipher invented by Sir Charles Wheatstone in 1854 was the first digram substitution cipher.

- It is named after Lord Playfair who promoted its use in diplomatic communication.
- In this cipher, a 5 x 5 grid is filled with letters of the English alphabet with the two letters I and J considered together.

Playfair Cipher 1/2

This substitution cipher invented by Sir Charles Wheatstone in 1854 was the first digram substitution cipher.

- It is named after Lord Playfair who promoted its use in diplomatic communication.
- In this cipher, a 5 x 5 grid is filled with letters of the English alphabet with the two letters I and J considered together.
- First, the grid is filled starting from the top left most cell with a short secret word without any repeating letters.

Playfair Cipher 1/2

This substitution cipher invented by Sir Charles Wheatstone in 1854 was the first digram substitution cipher.

- It is named after Lord Playfair who promoted its use in diplomatic communication.
- In this cipher, a 5 x 5 grid is filled with letters of the English alphabet with the two letters I and J considered together.
- First, the grid is filled starting from the top left most cell with a short secret word without any repeating letters.
- Thereafter, the remaining cells are filled with the letters of the alphabet in their natural order with letters already in the secret word skipped.

Playfair Cipher 2/2

- A digraphic substitution is then simulated by taking pairs of letters in the plaintext as two corners of a rectangle, and using the other two corners as the ciphertext.

Playfair Cipher 2/2

- A digraphic substitution is then simulated by taking pairs of letters in the plaintext as two corners of a rectangle, and using the other two corners as the ciphertext.
- A special rule handles double letters by inserting a pre-agreed extra letter to breakup the pairings falling in the same row or column.

Attacking Playfair Cipher

The technique encrypts pairs of letters (bigrams or digrams), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use.

Attacking Playfair Cipher

The technique encrypts pairs of letters (bigrams or digrams), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use.

- The Playfair is significantly harder to attack as there are more than 600 possible bigrams in contrast to only 26 monograms.

Attacking Playfair Cipher

The technique encrypts pairs of letters (bigrams or digrams), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use.

- The Playfair is significantly harder to attack as there are more than 600 possible bigrams in contrast to only 26 monograms.
- Therefore, to use frequency analysis of bigrams, a much larger amount of ciphertext needs to be captured by an attacker.

Playfair Cipher Example

The 5 x 5 grid with the secret keyword `CSE`

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

The encryption of plaintext `COMPUTER` would give the ciphertext `BKKRPUGX`

Rules

- If the two letters form a rectangle then take the letters on the horizontal opposite corner of the rectangle.
- If both letters are in the same column then take the letter below each one (going back to the top if at the bottom).
- If both letters are in the same row then take the letter to the right of each one (going back to the leftmost if at the rightmost position).

Permutation Cipher

While substitution ciphers have been used for the longest period, permutation ciphers also have a long history.

Permutation Cipher

While substitution ciphers have been used for the longest period, permutation ciphers also have a long history.

- Both these historical techniques, substitution and permutation, are now used in modern cipher systems.

Permutation Cipher

While substitution ciphers have been used for the longest period, permutation ciphers also have a long history.

- Both these historical techniques, substitution and permutation, are now used in modern cipher systems.
- Permutation ciphers require a block length n, which is typically a small value, and permutation σ.

Permutation Cipher

While substitution ciphers have been used for the longest period, permutation ciphers also have a long history.

- Both these historical techniques, substitution and permutation, are now used in modern cipher systems.
- Permutation ciphers require a block length n, which is typically a small value, and permutation σ.
- This results in a permutation group denoted as S_n where the permutation $\sigma \in S_n$ is the secret key (with block length n).

Permutation Cipher

While substitution ciphers have been used for the longest period, permutation ciphers also have a long history.

- Both these historical techniques, substitution and permutation, are now used in modern cipher systems.
- Permutation ciphers require a block length n, which is typically a small value, and permutation σ.
- This results in a permutation group denoted as S_n where the permutation $\sigma \in S_n$ is the secret key (with block length n).
- For example, with

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,4\,1\,3\,5 \end{pmatrix}$$

the plaintext word `HELLO` would be encrypted as ciphertext `LHLEO`.

Attacking Permutation Ciphers 1/2

If we receive a block of ciphertext, then a character frequency analysis where the result exactly matches the standard character frequency distribution would easily reveal if it has been created using a substitution cipher.

Attacking Permutation Ciphers 1/2

If we receive a block of ciphertext, then a character frequency analysis where the result exactly matches the standard character frequency distribution would easily reveal if it has been created using a substitution cipher.

- Then to successfully attack the cipher, we need to find the block length.

Attacking Permutation Ciphers 1/2

If we receive a block of ciphertext, then a character frequency analysis where the result exactly matches the standard character frequency distribution would easily reveal if it has been created using a substitution cipher.

- Then to successfully attack the cipher, we need to find the block length.
- If the plaintext has repeating character sequences that are aligned to the same block position, then there would be similar repeating character sequences in the ciphertext also.

Attacking Permutation Ciphers 1/2

If we receive a block of ciphertext, then a character frequency analysis where the result exactly matches the standard character frequency distribution would easily reveal if it has been created using a substitution cipher.

- Then to successfully attack the cipher, we need to find the block length.
- If the plaintext has repeating character sequences that are aligned to the same block position, then there would be similar repeating character sequences in the ciphertext also.
- This would help us to determine the block length (or possibly a multiple of the block length) by considering the distance between two repeating blocks.

Attacking Permutation Ciphers 2/2

- If we have two such different repeating character sequences, then finding the two distance values and computing their greatest common divisor would help find the block length.

Attacking Permutation Ciphers 2/2

- If we have two such different repeating character sequences, then finding the two distance values and computing their greatest common divisor would help find the block length.
- Once the block length is known, an exhaustive search can be used to deduce the permutation.

Epilogue - Historical Figures

Giovan Battista Bellaso

Giovan Battista Bellaso, was an Italian cryptologist born in 1505.[from Wikipedia]

Blaise de Vigenère

Blaise de Vigenère (1523 - 1596), born in Central France, was a French diplomat, cryptographer, translator and alchemist.[from Wikipedia]

Charles Babbage

Charles Babbage (1791 -1871), born in London, was a mathematician, philosopher, inventor and mechanical engineer. Babbage originated the concept of a digital programmable computer and hence considered by some to be "father of the computer". Babbage is credited with inventing the first mechanical computer known as Babbage's Analytical Engine.[from Wikipedia]

Charles Wheatstone

Sir Charles Wheatstone (1802 - 1875), was an English scientist and inventor of many scientific breakthroughs of the Victorian era, including the English concertina, the stereoscope (a device for displaying three-dimensional images), and the Playfair cipher (an encryption technique). However, Wheatstone is best known for his contributions in the development of the Wheatstone bridge, originally invented by Samuel Hunter Christie, which is used to measure an unknown electrical resistance, and as a major figure in the development of telegraphy.[from Wikipedia]

Friedrich Wilhelm Kasiski

Friedrich Wilhelm Kasiski (1805 - 1881), born in Kingdom of Prussia (present day Poland) was a German infantry officer, cryptographer and archaeologist. He wrote the book "Secret writing and the Art of Deciphering" (in German) that focused on cryptanalysis of poly-alphabetic substitution ciphers.[from Wikipedia]