Introduction to Cryptology

1.3 - Historical Ciphers

Federico Pintore

Mathematical Institute, University of Oxford (UK)

Michaelmas term 2020

Historical Encryption Schemes

Classical Cryptography mainly pursued secrecy.

Historical Encryption Schemes

Classical Cryptography mainly pursued secrecy.

Several *symmetric – key encryption schemes* were designed:

Historical Encryption Schemes

Classical Cryptography mainly pursued secrecy.

Several *symmetric – key encryption schemes* were designed:

- no clear definitions of security,
- no proofs of security.

Historical Encryption Schemes

Classical Cryptography mainly pursued secrecy.

Several *symmetric – key encryption schemes* were designed:

- no clear definitions of security,
- no proofs of security.

We review some of them, in order to learn some lessons.

Symmetric-key Encryption Schemes

Encryption scheme: $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \{E_e | e \in \mathcal{K}\}, \{D_d | d \in \mathcal{K}\})$

Symmetric-key Encryption Schemes

Encryption scheme: $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \{E_e | e \in \mathcal{K}\}, \{D_d | d \in \mathcal{K}\})$

A secret key $(e = d)$ is shared beforehand
by the communicating parties.

Symmetric-key Encryption Schemes

Encryption scheme: $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \{E_e | e \in \mathcal{K}\}, \{D_d | d \in \mathcal{K}\})$

A secret key $(e = d)$ is shared beforehand
by the communicating parties.

The sender encrypts a message, i.e. hides it, using E_e and obtains the ciphertext.

Symmetric-key Encryption Schemes

Encryption scheme: $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \{E_e | e \in \mathcal{K}\}, \{D_d | d \in \mathcal{K}\})$

A secret key $(e = d)$ is shared beforehand
by the communicating parties.

The sender encrypts a message, i.e. hides it, using E_e and obtains the ciphertext.

The receiver decrypts the ciphertext, i.e. unhides it, using D_d. They recover the original plaintext.

Caesar Cipher

- $\mathcal{M} = \mathcal{C} = \{\text{English words}\}$
- $\mathcal{K} = \{1, \ldots, 26\}$
- E_e shifts each letter of e positions to the right
- D_e shifts each letter of e positions to the left

Caesar Cipher

- $\mathcal{M} = \mathcal{C} = \{\text{English words}\}$
- $\mathcal{K} = \{1, \ldots, 26\}$
- E_e shifts each letter of e positions to the right
- D_e shifts each letter of e positions to the left

Example

- Plaintext: UNSAFE
- Key: $e = 3$
- Ciphertext: XQVDIH

Cryptanalysis of Caesar Cipher

Brute Force (try every possible key): $|\mathcal{K}|$ is only 26.

Cryptanalysis of Caesar Cipher

Brute Force (try every possible key): $|\mathcal{K}|$ is only 26.

Sufficient key-space principle: a secure symmetric-key encryption scheme must have a key space large enough to make a brute force attack infeasible ($|\mathcal{K}| \geq 2^{70}$).

Cryptanalysis of Caesar Cipher

Brute Force (try every possible key): $|\mathcal{K}|$ is only 26.

Sufficient key-space principle: a secure symmetric-key encryption scheme must have a key space large enough to make a brute force attack infeasible ($|\mathcal{K}| \geq 2^{70}$).

Is it a sufficient condition?

Substitution Cipher (mono-alphabetic)

- $\mathcal{M} = \mathcal{C} = \{\text{English words}\}$
- $\mathcal{K} = \{\text{permutations } p \text{ of the English alphabet}\}$
- E_p applies p to each letter of the plaintext
- D_p applies p^{-1} to each letter of the ciphertext

Substitution Cipher (mono-alphabetic)

- $\mathcal{M} = \mathcal{C} = \{\text{English words}\}$
- $\mathcal{K} = \{\text{permutations } p \text{ of the English alphabet}\}$
- E_p applies p to each letter of the plaintext
- D_p applies p^{-1} to each letter of the ciphertext

Example

- Plaintext: UNSAFE
- Key: p is the permutation sending A in T, . . . , E in N, F in L, . . . , N in R, . . . , S in O, . . . , U in H, . . .
- Ciphertext: HROTLN

Cryptanalysis of the Substitution Cipher

The brute force attack is not feasible, as $|\mathcal{K}| = 26! \approx 2^{88}$.

Cryptanalysis of the Substitution Cipher

The brute force attack is not feasible, as $|\mathcal{K}| = 26! \approx 2^{88}$.

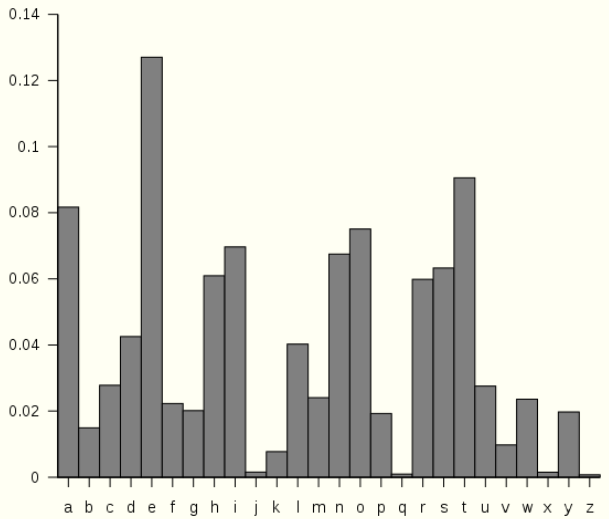
Frequency analysis can be performed:

Cryptanalysis of the Substitution Cipher

The brute force attack is not feasible, as $|\mathcal{K}| = 26! \approx 2^{88}$.

Frequency analysis can be performed:

- Frequency of English letters

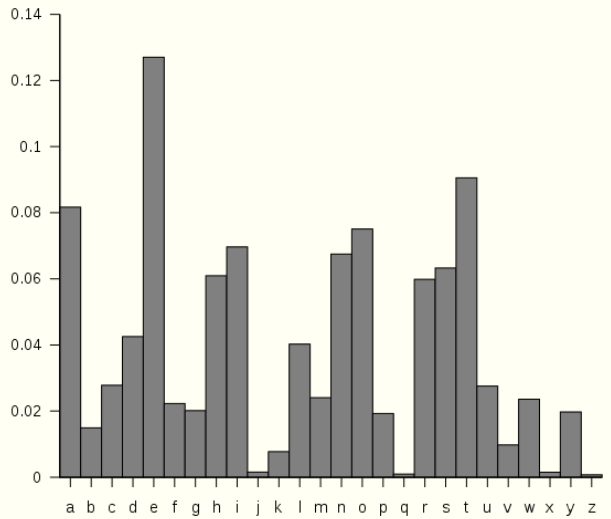


Cryptanalysis of the Substitution Cipher

The brute force attack is not feasible, as $|\mathcal{K}| = 26! \approx 2^{88}$.

Frequency analysis can be performed:

- Frequency of English letters



- Frequency of pairs (or more) of letters, e.g. digrams, trigrams, etc.

Vigenère Cipher (1553)

- $\mathcal{M} = \mathcal{C} = \{\text{English words}\}$
- $\mathcal{K} = \{(p_1, \ldots, p_t) | t \in \mathbb{N}\}$, where p_i is a circular permutation of the English alphabet
- $E_{(p_1,\ldots,p_t)}$ splits the plaintext into subsets of t letters and then applies $(p_1, \ldots, p_t)$
- $D_{(p_1,\ldots,p_t)}$ splits the ciphertext into subsets of t letters and then applies $(p_1^{-1}, \ldots, p_t^{-1})$

Vigenère Cipher (1553)

- $\mathcal{M} = \mathcal{C} = \{\text{English words}\}$
- $\mathcal{K} = \{(p_1, \ldots, p_t) | t \in \mathbb{N}\}$, where p_i is a circular permutation of the English alphabet
- $E_{(p_1,\ldots,p_t)}$ splits the plaintext into subsets of t letters and then applies $(p_1, \ldots, p_t)$
- $D_{(p_1,\ldots,p_t)}$ splits the ciphertext into subsets of t letters and then applies $(p_1^{-1}, \ldots, p_t^{-1})$

Example

- Plaintext: TOBEORNOTTOBE
- Key: $(p_1, \ldots, p_6)$, represented by CRYPTO (p_1 shifts each letter 3 positions to the right, ...)
- Ciphertext: VFZTHFPFRIHPG

Cryptanalysis of the Vigenère Cipher

When the value of t is known, break the ciphertext into blocks. Then each block is as it was encrypted by the Caesar cipher.

Cryptanalysis of the Vigenère Cipher

When the value of t is known, break the ciphertext into blocks. Then each block is as it was encrypted by the Caesar cipher.

When t is not known, use Kasiski method (Kasiski 1863) or the *index of coincidence method* to recover t.

Cryptanalysis of the Vigenère Cipher

When the value of t is known, break the ciphertext into blocks. Then each block is as it was encrypted by the Caesar cipher.

When t is not known, use Kasiski method (Kasiski 1863) or the *index of coincidence method* to recover t.

Important: when t is equal to number of letters of the plaintext (and the key is used only once), the above attacks do not work!

Lessons learned

Having a formal proof of security is essential.

Clear security definitions help with the design of cryptographic schemes, and they are required for security proofs.

History has shown that maintaining the design of a scheme secret is very difficult. Making the design public has several advantages (public scrutiny, standardisation, ...)

Further Reading I

Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis Guillou, Marie Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, and Soazig Guillou.
How to explain zero-knowledge protocols to your children.
In Advances in Cryptology—CRYPTO'89 Proceedings, pages 628–631. Springer, 1990.

Alice Silverberg.
Mathematics and cryptography: A marriage of convenience?
In Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT 2020, pages 3–9. Springer, Cham., 2020.

Further Reading II

Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, and Yarik Markov.
The first collision for full sha-1.
In Annual International Cryptology Conference - CRYPTO 2017, pages 570–596. Springer, Cham., 2017.