Public Key Cryptography

Lecture 1

A Brief Overview of Classical Cryptography

Index

Coordinates

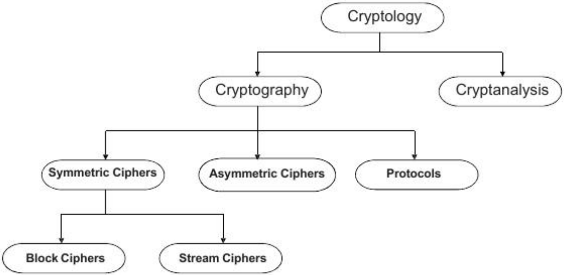
- Access to resources:
  Course *Public Key Cryptography* (password: pkc23)
  at https://moodle.cs.ubbcluj.ro, only with your scs.ubbcluj.ro address
  Team *Public Key Cryptography (2023-2024)* (code: hneh9g1)
  in MS Teams, only with your stud.ubbcluj.ro address
- Course contents:
  1. Classical cryptography
  2. Complexity and number theory
  3. Primality testing
  4. Factorization methods
  5. Public key cryptography
  6. Applications
- Assessment:
  1p for free
  4.5p for labs/projects
  4.5p for assignments
  1p for bonus assignment

Selective bibliography

- M. Cozzens, S.J. Miller, *The Mathematics of Encryption: An Elementary Introduction*, American Mathematical Society, 2013.
- S. Crivei, A. Marcus, C. Săcărea, C. Szántó, *Computational algebra with applications to coding theory and cryptography*, Ed. EFES, Cluj-Napoca, 2006.
- J. Daemen, V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer-Verlag, 2002.
- N. Ferguson, B. Schneier, *Practical Cryptography*, Wiley, 2003.
- C. Gherghe, D. Popescu, *Criptografie. Coduri. Algoritmi*, Univ. Bucureşti, 2005.
- D. Kahn, *The Codebreakers*, Macmillan, 1967.
- N. Koblitz, *A Course in Number Theory and Cryptography*, Springer, 1994.

- R. Lidl, G. Pilz, *Applied Abstract Algebra*, Springer-Verlag, 1998.
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. [http://www.cacr.math.uwaterloo.ca/hac]
- C. Paar, J. Pelzl, *Understanding Cryptography*, Springer, 2009.
- B. Schneier, *Applied Cryptography*, John Wiley and Sons, 1996.
- S. Singh, *The Code Book on CD-ROM* [http://www.simonsingh.net]
- S. Singh, *Cartea codurilor*, Humanitas, 2005.
- W. Stallings, *Cryptography and Network Security*, Prentice-Hall, 1999.
- D.R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.

Classification of cryptology



Fundamental aim of cryptography

To enable two people (Alice and Bob), to communicate over an insecure channel in such a way that an opponent (eavesdropper), Oscar (Eve), cannot understand what is being said.

Cryptosystem

Definition

Cryptosystem: a 5-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ such that:

- $\mathcal{P}$ is a finite set of possible *plaintext* characters/blocks.
- $\mathcal{C}$ is a finite set of possible *ciphertext* characters/blocks.
- $\mathcal{K}$ is a finite set of possible keys.
- For each $K \in \mathcal{K}$, there is an *encryption rule* $e_K \in \mathcal{E}$ and a *decryption rule* $d_K \in \mathcal{D}$. Each $e_K : \mathcal{P} \to \mathcal{C}$ and $d_K : \mathcal{C} \to \mathcal{P}$ are functions such that $d_K(e_K(x)) = x$ for every $x \in \mathcal{P}$.

Each encryption function e_K must be injective.
If $\mathcal{P} = \mathcal{C}$, then each e_K is a permutation.
Each e_K and each d_K should be efficiently computable (given K).

The Shift (Caesar) Cipher

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ (an *alphabet*)
- $\forall K \in \mathbb{Z}_n$, $\forall x, y \in \mathbb{Z}_n$,
  $e_K(x) = x + K \pmod{n}, \quad d_K(y) = y - K \pmod{n}.$

Example. $n = 27$, $K = 10$.

_	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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- Plaintext: first_example
- Numerical: 6 9 18 19 20 0 5 24 1 13 16 12 5
- Encryption: 16 19 1 2 3 10 15 7 11 23 26 22 15
- Ciphertext: PSABCJOGKWZVO

The Substitution Cipher

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$
- $\mathcal{K} = \{\sigma : \mathbb{Z}_n \to \mathbb{Z}_n \mid \sigma \text{ is bijective}\}$ (permutations)
- $\forall \sigma \in \mathcal{K}$, $\forall x, y \in \mathbb{Z}_n$: $e_\sigma(x) = \sigma(x)$, $d_\sigma(y) = \sigma^{-1}(y)$.

Example. $n = 27$, encryption function e_σ given by:

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

- Ciphertext: BZWFQLPZGYMJSZ
- Decryption function d_σ given by:

_	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
u	y	s	w	q	z	o	x	r	v	p	t	d	m	b	k	_	n	h	l	f	j	i	c	g	a	e

- Plaintext: second_example

The Affine Cipher

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$
- $\mathcal{K} = \{(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n \mid gcd(a, n) = 1\}$
- $\forall K = (a, b) \in \mathcal{K}, \forall x, y \in \mathbb{Z}_n$:
  $e_K(x) = ax + b \pmod{n}$, $d_K(y) = a^{-1}(y - b) \pmod{n}$.

Note that e_K is injective $\iff gcd(a, n) = 1$.

Example. $n = 27$, $K = (7, 5)$. Hence $e_K(x) = 7x + 5$.
We have $7^{-1} \pmod{27} = 4$ (see the Extended Euclidean Algorithm or determine x such that $7x = 1 \pmod{27}$).
Then $d_K(y) = 4(y - 5) = 4y + 7$.

- Plaintext: hey
- Numerical: 8 5 25
- Encryption: 7 13 18
  $(7 \cdot 8 + 5 \pmod{27}, 7 \cdot 5 + 5 \pmod{27}, 7 \cdot 25 + 5 \pmod{27})$
- Ciphertext: GMR

The Belaso (Vigenère) Cipher

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_n)^m$
- $\forall K = (k_1, \ldots, k_m) \in \mathcal{K}$, $\forall (x_1, \ldots, x_m), (y_1, \ldots, y_m) \in (\mathbb{Z}_n)^m$:
  $e_K(x_1, \ldots, x_m) = (x_1 + k_1, \ldots, x_m + k_m)$,
  $d_K(y_1, \ldots, y_m) = (y_1 - k_1, \ldots, y_m - k_m)$
  (everything mod n).

Example. $n = 27$, $m = 6$, keyword CIPHER, hence $K = (3, 9, 16, 8, 5, 18)$.

- Plaintext: computational
- Numerical: 3 15 13 16 21 20 /1 20 9 15 14 1 /12
- Encryption: 6 24 2 24 26 11 /4 2 25 23 19 19 /15
- Ciphertext: FXBXZKDBYWSSO

The Hill Cipher

- $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_n)^m$
- $\mathcal{K} = \{K \in M_m(\mathbb{Z}_n) \mid K \text{ invertible and } gcd(det\, K, n) = 1\}$
- $\forall K \in \mathcal{K}$, $\forall x, y \in (\mathbb{Z}_n)^m$: $e_K(x) = xK$, $d_K(y) = yK^{-1}$ (everything mod n).

Note that e_K is injective $\iff gcd(det\, K, n) = 1$.

Example. $n = 27$, $m = 2$, $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$, hence $K^{-1} = \begin{pmatrix} 20 & 8 \\ 3 & 16 \end{pmatrix}$.
Note that $K \cdot K^{-1} = K^{-1} \cdot K = I_2$ (everything mod n).

- Plaintext: four
- Numerical: 6 15 /21 18
- Encryption: 3 18 /15 24
  $\left[(6\ 15)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (3\ 18), \quad (21\ 18)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (15\ 24)\right]$
- Ciphertext: CROX

The Permutation Cipher

- $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_n)^m$
- $\mathcal{K} = \{\sigma : \{1,\ldots,m\} \to \{1,\ldots,m\} \mid \sigma \text{ is bijective}\}$ (permutations)
- $\forall \sigma \in \mathcal{K}$, $\forall (x_1,\ldots,x_m), (y_1,\ldots,y_m) \in (\mathbb{Z}_n)^m$:
  $e_\sigma(x_1,\ldots,x_m) = (x_{\sigma(1)},\ldots,x_{\sigma(m)})$,
  $d_\sigma(y_1,\ldots,y_m) = (y_{\sigma^{-1}(1)},\ldots,y_{\sigma^{-1}(m)})$.

Example. $n = 27$, $m = 5$, $\sigma = \binom{1\ 2\ 3\ 4\ 5}{2\ 4\ 5\ 3\ 1}$.
We have $\sigma^{-1} = \binom{1\ 2\ 3\ 4\ 5}{5\ 1\ 4\ 2\ 3}$.

- Plaintext: computational
  (compu /tatio /nal__)
- Encryption: OPUMC /AIOTT /A__LN
- Ciphertext: OPUMCAIOTTA__LN

Classification

Definition

Block cipher: each plaintext element (block) is encrypted using the same key. *Stream cipher*: not a block cipher.

All previous examples are block ciphers.

Definition

Monoalphabetic cipher: each character is mapped to a unique character. *Polyalphabetic cipher*: not a monoalphabetic cipher.

Monoalphabetic: shift cipher, substitution cipher, affine cipher.

- $\{\text{shift}\} \subseteq \{\text{affine}\} \subseteq \{\text{substitution}\}$

Polyalphabetic: Belaso cipher, Hill cipher, permutation cipher.

- $\{\text{permutation}\} \subseteq \{\text{Hill}\}$

Cryptanalysis

Necessary characteristic of a cryptosystem

An opponent (Oscar), upon seeing a ciphertext string, should be unable to determine the key K or the plaintext string.

Definition

Cryptanalysis: the process of attempting to compute the key K, given a string of ciphertext.

General assumption

The opponent (Oscar) knows the cryptosystem being used.

- An elementary type of attack is the *exhaustive key search attack*, when Oscar tries all the possible keys until a meaningful plaintext is obtained.
- Another type of attack is the *ciphertext-only attack*, when Oscar possesses a string of ciphertext.

Cryptanalysis (cont.)

- Number of keys for previous ciphers for an alphabet with $n = 27$:
  - Shift cipher: 27
  - Substitution cipher: 27!
  - Affine cipher: $\varphi(27) \cdot 27 = 18 \cdot 27 = 486$
    (φ is the Euler function)
  - Vigenère cipher: 27^m
  - Permutation cipher: m!
- Let us consider a couple of examples of ciphertext-only attacks.

  Assume that the plaintext string is ordinary English text, without punctuation or blanks. This makes the decryption more difficult.

  Use statistical properties of the English language.

Cryptanalysis of the Substitution Cipher

Example. Consider the following ciphertext:

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBJY RBSZI
QLZRL HOIZQ GBYLH
```

The most common letters are B, I, L, Y, H, occurring 26, 25, 24, 23, and 20 times respectively.

Cryptanalysis of the Substitution Cipher (cont.)

Frequencies of letters in English text cf. `http://www.cryptograms.org/letter-frequencies.php`.

1	e	12.58%	14	m	2.56%
2	t	9.09%	15	f	2.35%
3	a	8.00%	16	w	2.22%
4	o	7.59%	17	g	1.98%
5	i	6.92%	18	y	1.90%
6	n	6.90%	19	p	1.80%
7	s	6.34%	20	b	1.54%
8	h	6.24%	21	v	0.98%
9	r	5.96%	22	k	0.74%
10	d	4.32%	23	x	0.18%
11	l	4.06%	24	j	0.15%
12	u	2.84%	25	q	0.12%
13	c	2.58%	26	z	0.08%

Cryptanalysis of the Substitution Cipher (cont.)

It is reasonable to assume that the plaintext letters T and E correspond to some of these most common letters B, I, L, Y, H.

If we assume that E was encrypted to B and T was encrypted to I, we can make the following substitutions:

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
    t     t         e   te t   e  t       ee       t     et    e
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
t                    e     e        t  e    t   t     tt t    e e
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
 t      t     et      t         e e          e   t        t    e
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBJY RBSZI
       e       e   e t   t        e       e     e  e    e    e  e
QLZRL HOIZQ GBYLH
        t    e
```

Cryptanalysis of the Substitution Cipher (cont.)

There is something strange about this substitution: nowhere does the pattern T_E appear, which would mean that the word "the" never appears in the passage.

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
    t     t         e   te t   e  t       ee       t     et    e
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
t                    e     e        t  e    t   t     tt t    e e
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
 t      t     et      t         e e          e   t        t    e
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBJY RBSZI
       e       e   e t   t        e       e     e  e    e    e  e
QLZRL HOIZQ GBYLH
        t    e
```

Switching T and E gives

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
    e     e         t   et e   t  e       tt       e     te    t
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
e                    t     t        e  t    e   e     ee e    t t
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
 e      e     te      e         t t          t   e        e     t
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBJY RBSZI
       t       t   t e   e        t       t     e  t    t    t  e
QLZRL HOIZQ GBYLH
        e    t
```

There are now four instances of the pattern T_E: in the fifth block on the first line (ciphertext BOI), straddling the last block of the first line and the first block of the second line (ciphertext BTI), straddling the last block of the second line and the first block of the third line (ciphertext BTI), and in the fourth block of the fourth line (ciphertext BTI).

Cryptanalysis of the Substitution Cipher (cont.)

Based on these occurrences, it seems reasonable to assume that T in the ciphertext corresponds to H in the plaintext and that the first instance BOI was just a coincidence (otherwise our long phrase would only have one "the").

Filling in this substitution, we get the following:

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
    e     e         t   et e   t  e       tt      he     te    th
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
e           h        th    t        e  t    e h eh    ee e    t t
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
he     he     te      e         t t h        t   e        e    t
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBYJ RBSZI
       t     h t   the   e        t h   h t     e  th   t    t  e
QLZRL HOIZQ GBYLH
        e    t
```

Cryptanalysis of the Substitution Cipher (cont.)

Continuing now with frequency analysis, the most common ciphertext letters for which we have not assigned a substitution are L, Y, and H. Referring to the frequency table, the most common English letters after e and t are a, o, and i. Notice, however, that the pattern LL occurs three times in the ciphertext: of the letters a, o, and i, only o appears commonly as a double letter in English, so it is natural to guess that L was substituted for O:

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
    e     e         to  et e   t  e  o    tt       he     te  o th
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
e        o  h       oth    to  oo   eo t    e h eh    ee e    tot
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
he oo  he     te      e         t t h   o    t   e o   o  e    t
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBJY RBSZI
o       t     h t   the   eo    oo t ho  h t     e  th o t    t  e
QLZRL HOIZQ GBYLH
 o  o   e     t o
```

Cryptanalysis of the Substitution Cipher (cont.)

We can also try frequency analysis on blocks of letters. E.g., the three letter block YHC occurs five times in the ciphertext, more than any other triple. The most common English "trigrams" are *the*, *and*, and *ing*. Since our guesses so far rule out the *the*, it is natural to make the substitutions Y→A, H→N, and C→D:

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
  a e     e danna ndtod et e   ta e  o  a ttand   he   a te  onth
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
e  n   n o  h  an dnoth andto  oon  eo t  a e h eh    ee e  antot
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
he oo  he   a te      e   and   tat h  no    t   e o   o  e     t
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBJY RBSZI
on an at n   h ta  the   eo     oo t ho  h t     e  th o t    t  e
QLZRL HOIZQ GBYLH
 o  o n e    tyon
```

Unfortunately, there are indications that this last set of substitutions may be incorrect. For example, in the first line we now have have the blocks EDANNANDTODET and NOTHANDTO in the plaintext, on the first and second lines, respectively. Both of these blocks would seem more reasonable if A and D were replaced with I and G, respectively, suggesting that perhaps the ciphertext triple YHC corresponded to the trigram ING and not AND. Making these changes gives us:

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
  i e     e  inni ngtog et e   ti e  o  i tting   he   i te  onth
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
e  n   n o  h  in gnoth ingto  oon  eo t  i e h eh    ee e  intot
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
he oo  he   i te      e   ing   tit h  no    t   e o   o  e     t
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBJY RBSZI
on in it n   h ti  the   eo    oo t ho  h t     e  th o t    t  e
QLZRL HOIZQ GBYLH
 o  o n e    tyon
```

Cryptanalysis of the Substitution Cipher (cont.)

Note the troublesome blocks are now EGINNINGTOGET and NOTHINGTO. At this point, we are basically playing hangman, trying to guess more substitutions by what is needed to make the revealed phrases words. For example, EGINNINGTOGET seems like it could be BEGINNINGTOGET, suggesting the substitution K→B, while NOTHINGTO O could be NOTHINGTODO, suggesting the substitution E→D. Making these substitutions yields:

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
  i e    be ginni ngtog et e   ti e do  i tting b he   i te  onth
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
eb n   ndo h   in gnoth ingto doon  eo t  i e h eh d  ee ed intot
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
heboo  he  i te      e  ding b tit h  no    t i e o  o  e     t
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBJY RBSZI
on in it nd  h ti  the   eo   boo t ho  h t    e  th o t   t  e
QLZRL HOIZQ GBYLH
 o  o n e   tyon
```

Cryptanalysis of the Substitution Cipher (cont.)

Spanning the end of the second line and beginning of the third, the plaintext block INTOTHEBOO suggests the substitution U→K. In the third line, we have the plaintext INGB_TIT. The ING almost certainly represents the end of a word. It seems clear that the blank must be a vowel, and U seems the most likely candidate. The substitutions U→K and S→U give

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
 i e     be ginni ngtog et e   ti e do  i tting b he   i te  onth
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
eb nk  ndo  h  in gnoth ingto doon  eo t  i e h eh d  ee ed intot
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
heboo khe   i te      e  ding butit h  no    tu  e o   o  e     t
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBJY RBSZI
on in it nd  h ti  theu  eo   bookt ho  h t     e  th o t    t  e
QLZRL HOIZQ GBYLH
 o  o n e    tyon
```

We could choose to concentrate on many different parts of the message. Moving on, another possibility presents itself on the first line, as TI_EDO__ITTING becomes TIREDOFSITTING under the substitutions Z→R, P→F, and Q→S. On the second line, ON_EO_T_I_E becomes ONCEORTWICE under the substitutions R→C, Z→R, and N→W. These five substitutions bring us to:

```
GAYRI NGQKI CYHHY HCBLC IBOIZ VBYZI ELPQY BBYHC KVTIZ QYQBI ZLHBT
  ice   sbe ginni ngtog et er  tire dofsi tting b her siste ronth
IKGHU GHELP TGOYH CHLBT YHCBL ELLHR ILZBN YRIQT ITGEJ IIJIE YHBLB
eb nk  ndof h  in gnoth ingto doonc eortw icesh eh d  ee ed intot
TIKLL UTIZQ YQBIZ NGQZI GEYHC KSBYB TGEHL JYRBS ZIQLZ RLHOI ZQGBY
heboo khers ister   sre  ding butit h  no   rtu resor co  e  rs t
LHQYH YBGHE NTGBY QBTIS QILPG KLLUB TLSCT BGAYR INYBT LSBJY RBSZI
onsin it nd  h ti stheu seof  bookt ho  h t   c e  th o t   ct re
QLZRL HOIZQ GBYLH
sorco n ers  tyon
```

Cryptanalysis of the Substitution Cipher (cont.)

Now one easily gets the whole plaintext:

```
ALICE WASBE GINNI NGTOG ETVER YTIRE DOFSI TTING BYHER SISTE RONTH
EBANK ANDOF HAVIN GNOTH INGTO DOONC EORTW ICESH EHADP EEPED INTOT
HEBOO KHERS ISTER WASRE ADING BUTIT HADNO PICTU RESOR CONVE RSATI
ONSIN ITAND WHATI STHEU SEOFA BOOKT HOUGH TALIC EWITH OUTPI CTURE
SORCO NVERS ATION
```

ALICE WAS BEGINNING TO GET VERY TIRED OF SITTING BY HER SISTER ON THE BANK AND OF HAVING NOTHING TO DO ONCE OR TWICE SHE HAD PEEPED INTO THE BOOK HER SISTER WAS READING BUT IT HAD NO PICTURES OR CONVERSATIONS IN IT AND WHAT IS THE USE OF A BOOK THOUGHT ALICE WITHOUT PICTURES OR CONVERSATION (Lewis Carroll)

Some Modern Block Ciphers

- Enigma and Hagelin machines (starting with 1920s) implement polyalphabetic substitution ciphers with long periods. They generate sequences of long keys, not so random as they might seem, and so they are vulnerable.

- Lucifer cipher, Feistel ciphers: 1970's
- DES (Data Encryption Standard): 1977
- IDEA (International Data Encryption Algorithm): 1991
- RC5: 1994
- AES (Advanced Encryption Standard): 2002

Selective Bibliography

- M. Cozzens, S.J. Miller, *The Mathematics of Encryption: An Elementary Introduction*, American Mathematical Society, 2013.
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. [http://www.cacr.math.uwaterloo.ca/hac]
- C. Paar, J. Pelzl, *Understanding Cryptography*, Springer, 2009.