Permutation polynomials over finite fields and their application to cryptography

Daniele Bartoli

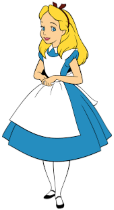
University of Perugia
Department of Mathematics and Computer Science

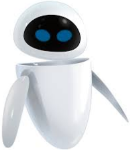
City Tech - February 13, 2020

OUTLINE

- Cryptography: what's that?
- Symmetric Cryptography
- Public key Cryptography
- Permutation Polynomials

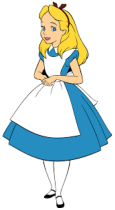
Cryptography: what's that?

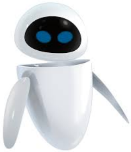




Alice would like to send Bob a message in a way that Eve is not able to understand it

Cryptography: what's that?



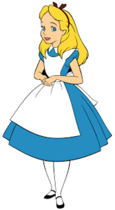


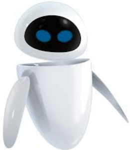
Alice would like to send Bob a message in a way that Eve is not able to understand it

- Fundamental since the ancient times
- Now it is even more important
  - Buy/sell things online
  - Wireless devices



Cryptography: what's that?



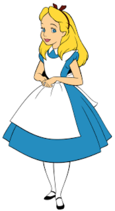


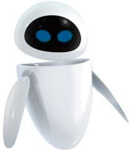
Alice would like to send Bob a message in a way that Eve is not able to understand it

- Fundamental since the ancient times
- Now it is even more important
  - Buy/sell things online
  - Wireless devices

"Verba volant, scripta manent"

Cryptography: what's that?





Alice would like to send Bob a message in a way that Eve is not able to understand it

- Fundamental since the ancient times
- Now it is even more important
  - Buy/sell things online
  - Wireless devices



"Verba volant, ~~scripta~~ bits manent"

Information is just numbers

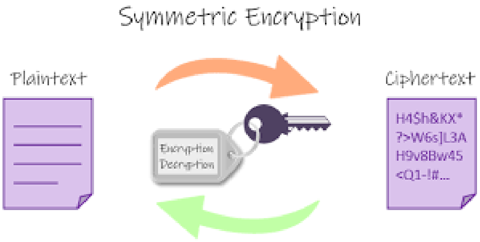
In our digital world information is represented by strings of ciphers

Information is just numbers

In our digital world information is represented by strings of ciphers

How to hide a number?

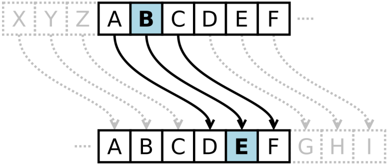
CLASSIC (SYMMETRIC) CRYPTOGRAPHY



- PLAINTEXT: 'true' message that Alice wants to send Bob, Everybody can understand it
- CYPHERTEXT: message after encryption
- ENCRYPTION: process which transforms plaintext into ciphertext
- DECRYPTION: process which transforms ciphertext into plaintext again
- CRYPTOGRAPHIC KEY: 'piece of information' that determines the output of a cryptographic algorithm

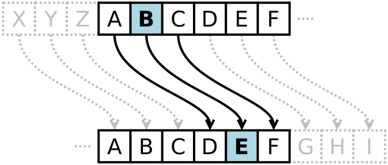
An example: CAESAR CIPHER

Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.
(Svetonio, De Vita Caesarum)



An example: CAESAR CIPHER

Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.
(Svetonio, De Vita Caesarum)



$$\text{science} \mapsto \text{vfnhqfh}$$

An example: CAESAR CIPHER

From a mathematical point of view . . .

1. Letters $\mapsto$ Numbers

A	B	C	D	. . .	X	Y	Z
0	1	2	3	. . .	23	24	25

2. ENCRYPTION: X is sent to $X + 3 \pmod{26}$

3. Key?

An example: CAESAR CIPHER

From a mathematical point of view ...

1. Letters $\mapsto$ Numbers

A	B	C	D	...	X	Y	Z
0	1	2	3	...	23	24	25

2. ENCRYPTION: X is sent to $X + 3 \pmod{26}$

3. Key? 3

An old way. . . still used by Mafia

(Provenzano's "pizzini")

Provenzano frowned upon the use of telephones and issued orders and communications (even to his family) through small, hand-delivered notes called pizzini. Provenzano used a version of the Caesar cipher, used by Julius Caesar in wartime communications.
WIKIPEDIA

CAESAR CIPHER: problems

- Few possible Keys: possible brute-force attack

- CAESAR CIPHER is just a substitution: every letter is encrypted always in the same way. Possible frequency analysis

CAESAR CIPHER: problems

- Few possible Keys: possible brute-force attack

- CAESAR CIPHER is just a substitution: every letter is encrypted always in the same way. Possible frequency analysis

Frequency analysis is based on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. Moreover, there is a characteristic distribution of letters that is roughly the same for almost all samples of that language.

CAESAR CIPHER: problems

- Few possible Keys: possible brute-force attack
- CAESAR CIPHER is just a substitution: every letter is encrypted always in the same way. Possible frequency analysis

Frequency analysis is based on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. Moreover, there is a characteristic distribution of letters that is roughly the same for almost all samples of that language.

Possible solution:
Use a word, a sentence, or a book as key

How to use a word as key

S	E	E	Y	O	U	T	O	M	O	R	R	O	W
18	4	4	24	14	20	19	14	12	14	17	17	14	22
H	E	L	L	O	H	E	L	L	O	H	E	L	L
7	4	11	11	14	7	4	11	11	14	7	4	11	11
25	8	15	9	2	1	23	25	23	2	24	21	25	7
Z	I	P	J	C	B	X	Z	X	C	Y	V	Z	H

The longer the key, the more difficult the frequency analysis

How to use a word as key

S	E	E	Y	O	U	T	O	M	O	R	R	O	W
18	4	4	24	14	20	19	14	12	14	17	17	14	22
H	E	L	L	O	H	E	L	L	O	H	E	L	L
7	4	11	11	14	7	4	11	11	14	7	4	11	11
25	8	15	9	2	1	23	25	23	2	24	21	25	7
Z	I	P	J	C	B	X	Z	X	C	Y	V	Z	H

The longer the key, the more difficult the frequency analysis

1. key: sequence of numbers
2. same letter is moved to different letters depending on its position

How to use a word as key

S	E	E	Y	O	U	T	O	M	O	R	R	O	W
18	4	4	24	14	20	19	14	12	14	17	17	14	22
H	E	L	L	O	H	E	L	L	O	H	E	L	L
7	4	11	11	14	7	4	11	11	14	7	4	11	11
25	8	15	9	2	1	23	25	23	2	24	21	25	7
Z	I	P	J	C	B	X	Z	X	C	Y	V	Z	H

The longer the key, the more difficult the frequency analysis

1. key: sequence of numbers
2. same letter is moved to different letters depending on its position
3. if the key is as long as the message then the cipher is perfect

A perfect cipher is defined as a cipher in which, if an attacker intercepts the ciphertext, it receives no information about the message being sent.

So . . . we are done!!!

If we can use a key as long as the message, our method is perfect! But. . .

So . . . we are done!!!

If we can use a key as long as the message, our method is perfect! But. . .

ALICE and BOB must share the key!

So . . . we are done!!!

If we can use a key as long as the message, our method is perfect! But. . .

ALICE and BOB must share the key!

HOW TO SHARE THE KEY?

So . . . we are done!!!

If we can use a key as long as the message, our method is perfect! But. . .

ALICE and BOB must share the key!

HOW TO SHARE THE KEY?

Sometimes this is really impossible. . .

So . . . we are done!!!

If we can use a key as long as the message, our method is perfect! But. . .

ALICE and BOB must share the key!

HOW TO SHARE THE KEY?

Sometimes this is really impossible. . .

- WHATSAPP cannot understand what ALICE and BOB say
- Everybody can talk with everybody
- More than 10^9 customers!!!

Solution: ASYMMETRIC CRYPTOGRAPHY

- TWO different keys: one key to encrypt, one key to decrypt
- key to encrypt is PUBLIC: everybody can use it
- key to decrypt is PRIVATE: only who receive the cypher-text knows it
- IMPOSSIBLE to recover PRIVATE key for PUBLIC key

IMPOSSIBLE TO GO BACK

Main tool: use something which makes not possible for EVE to know PRIVATE key of BOB knowing his PUBLIC key

What do we mean for IMPOSSIBLE?

COMPUTATIONALLY impossible, i.e. impossible in a useful amount of time

ACTIONS impossible to invert: some examples

To know the phone number of a person using the phone book knowing his/her name: $\Longrightarrow$ EASY

To know the name of a person using the phone book knowing his/her phone number: $\Longrightarrow$ IMPOSSIBLE!

ACTIONS impossible to invert: some examples

To prepare a cake
following its recipe: $\Longrightarrow$ "EASY"

To know the recipe of a cake
after eating the cake $\Longrightarrow$ IMPOSSIBLE!

?

ACTIONS impossible to invert: some examples

To prepare a cake
following its recipe: $\Longrightarrow$ "EASY"

To know the recipe of a cake
after eating the cake $\Longrightarrow$ IMPOSSIBLE!

?

Do you the most secret recipe in the world?

ACTIONS impossible to invert: some examples

To prepare a cake following its recipe: $\Longrightarrow$ "EASY"

To know the recipe of a cake after eating the cake $\Longrightarrow$ IMPOSSIBLE!

?

Do you the most secret recipe in the world?

ACTIONS impossible to invert: mathematics

Discrete Logarithm (Logarithm over finite fields)

ACTIONS impossible to invert: mathematics

Discrete Logarithm (Logarithm over finite fields)

- Real Logarithm is easy to compute or to approximate

$$2^{13} = 8192, \qquad 2^{14} = 16384 \qquad \Longrightarrow \log_2(13321) \in]13, 14[$$

- Discrete Logarithm is hard to compute
  the best strategy is to try all the possibilities until it is right

Finite fields

Definition (roughly. . .)

A finite set $\mathbb{F}$ with two operations $\oplus$ and $\odot$ satisfying "nice" rules (as in the real case)

- Associativity
- Commutativity
- Existence neutral element
- Existence of the inverse (opposite) for each non-zero element

Finite fields: an example

$$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$$

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$$A \oplus B = C \pmod 5 \qquad A \odot B = C \pmod 5$$

Diffie-Hellman's protocol

Alice wants to send Bob a message

Alice and Bob want to share a secret which will be their secret key (in symmetric cryptography)

Diffie-Hellman's protocol

- Chooses a number A
- Chooses an exponent b
- Computes A^b
- Bob publishes A and A^b
- Bob keeps b secret

- Chooses an exponent c
- Computes A^c
- Sends Bob A^c

Diffie-Hellman's protocol

- Chooses a number A
- Chooses an exponent b
- Computes A^b
- Bob publishes A and A^b
- Bob keeps b secret

- Chooses an exponent c
- Computes A^c
- Sends Bob A^c

Alice and Bob both know $A^{bc} = (A^c)^b = (A^b)^c$

Diffie-Hellman's protocol

- Chooses a number A
- Chooses an exponent b
- Computes A^b
- Bob publishes A and A^b
- Bob keeps b secret

- Chooses an exponent c
- Computes A^c
- Sends Bob A^c

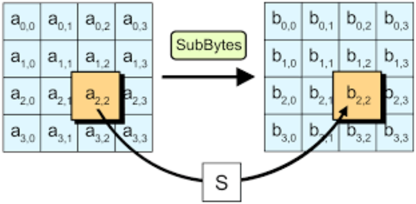
Alice and Bob both know $A^{bc} = (A^c)^b = \left(A^b\right)^c$

Eve can read A, A^b, A^c *but cannot compute* A^{bc}*!*

The importance of permutations: AES

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001

- AES has been adopted by the U.S. government and is now used worldwide
- It supersedes the Data Encryption Standard (DES)
- AES is a symmetric-key algorithm
- It is organized in rounds divided into different steps
- One of these steps is a (non-linear) substitution: S-Box



Tools from finite fields: permutation polynomials

In DES or AES some in some of the rounds there are permutations over finite fields

Definition (Permutation Polynomial)

A Permutation Polynomial is a polynomial $f(x)$ with coefficients in $\mathbb{F}_q$ such that $c \mapsto f(c)$ is a permutation (invertible) of $\mathbb{F}_q$

$$\mathbb{F}_5 \qquad f(x) = 3x^3 + 2x^2 + x + 4 \in \mathbb{F}_5[x]$$

Remark

Since $\mathbb{F}_q$ is finite it is enough to check if $c \mapsto f(c)$ is injective (or surjective) or not

Permutation polynomials

Example

Consider $f(x) = x + 3 \in \mathbb{F}_5[x]$

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Permutation polynomials

Example

Consider $f(x) = x + 3 \in \mathbb{F}_5[x]$

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$f(x) = x + 3 \in \mathbb{F}_5[x]$ is a Permutation Polynomial

Exercise

Prove that any polynomial

$$f(x) = Ax + B \in \mathbb{F}_5[x], \quad with \quad A, B \in \mathbb{F}_5, \quad A \neq 0$$

is a Permutation Polynomial

Permutation polynomials

Example

Consider $f(x) = x^2 \in \mathbb{F}_5[x]$

$$f(0) = 0, \quad f(1) = 1, \quad f(2) = 4, \quad f(3) = 4, \quad f(4) = 1$$

it is not a Permutation Polynomial

Known families of PP

- Monomials: x^n PP $\iff (n, q-1) = 1$
- Dickson :

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i} \in \mathbb{F}_q[x]$$

$$\left(\forall x \neq 0 \qquad D_n\left(x + \frac{a}{x}, a\right) = x^n + \left(\frac{a}{x}\right)^n\right)$$

PP $\iff (n, q^2 - 1) = 1$

- Linearized polynomials

$$\sum_{s=0}^{n-1} a_s x^{q^s} \in \mathbb{F}_{q^n}[x] \text{ PP } \iff \det \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix} \neq 0$$

Permutation Polynomials and Curves over finite fields

Definition (Affine plane)

$$AG(2, q) := \{(a, b) : a, b \in \mathbb{F}_q\}$$

Permutation Polynomials and Curves over finite fields

Definition (Affine plane)

$$AG(2,q) := \{(a,b) : a,b \in \mathbb{F}_q\}$$

Example ($AG(2,5)$)

$$\begin{array}{ccccc} (4,0) & (4,1) & (4,2) & (4,3) & (4,4) \\ (3,0) & (3,1) & (3,2) & (3,3) & (3,4) \\ (2,0) & (2,1) & (2,2) & (2,3) & (2,4) \\ (1,0) & (1,1) & (1,2) & (1,3) & (1,4) \\ (0,0) & (0,1) & (0,2) & (0,3) & (0,4) \end{array}$$

Definition (Curve)

$\mathcal{C}$ in $AG(2,q)$ Curve $\iff$ polynomial $F(X,Y) \in \mathbb{F}_q[X,Y]$

Permutation Polynomials and Curves over finite fields

Definition (Affine plane)

$$AG(2, q) := \{(a, b) : a, b \in \mathbb{F}_q\}$$

Example ($AG(2, 5)$)

$$\begin{matrix} (4,0) & (4,1) & (4,2) & (4,3) & (4,4) \\ (3,0) & (3,1) & (3,2) & (3,3) & (3,4) \\ (2,0) & (2,1) & (2,2) & (2,3) & (2,4) \\ (1,0) & (1,1) & (1,2) & (1,3) & (1,4) \\ (0,0) & (0,1) & (0,2) & (0,3) & (0,4) \end{matrix}$$

Definition (Curve)

$\mathcal{C}$ in $AG(2, q)$ Curve $\iff$ polynomial $F(X, Y) \in \mathbb{F}_q[X, Y]$

$$2X + 7Y^2 + 3 \iff 4X + 14Y^2 + 6$$

Permutation Polynomials and Curves over finite fields

$$f(x) \in \mathbb{F}_q[x] \Longrightarrow \mathcal{C}_f : f(X) - f(Y) = 0$$

Permutation Polynomials and Curves over finite fields

$$f(x) \in \mathbb{F}_q[x] \Longrightarrow \mathcal{C}_f : f(X) - f(Y) = 0$$

Consider $f(x) = x^2 \in \mathbb{F}_5[x]$

Permutation Polynomials and Curves over finite fields

$$f(x) \in \mathbb{F}_q[x] \Longrightarrow \mathcal{C}_f : f(X) - f(Y) = 0$$

Consider $f(x) = x^2 \in \mathbb{F}_5[x] \mapsto$ Not a PP

$$\mathcal{C}_f \; : \; X^2 - Y^2 = 0$$

Permutation Polynomials and Curves over finite fields

$$f(x) \in \mathbb{F}_q[x] \Longrightarrow \mathcal{C}_f : f(X) - f(Y) = 0$$

Consider $f(x) = x^2 \in \mathbb{F}_5[x] \mapsto$ Not a PP

$$\mathcal{C}_f \ : \ X^2 - Y^2 = 0$$

$$\begin{array}{ccccc}
(4,0) & (4,1) & (4,2) & (4,3) & (4,4) \\
(3,0) & (3,1) & (3,2) & (3,3) & (3,4) \\
(2,0) & (2,1) & (2,2) & (2,3) & (2,4) \\
(1,0) & (1,1) & (1,2) & (1,3) & (1,4) \\
(0,0) & (0,1) & (0,2) & (0,3) & (0,4)
\end{array}$$

Permutation Polynomials and Curves over finite fields

Consider $f(x) = x^3 \in \mathbb{F}_5[x]$

Permutation Polynomials and Curves over finite fields

Consider $f(x) = x^3 \in \mathbb{F}_5[x] \mapsto$ it is a PP since $(3, q-1) = (3, 4) = 1$

$$\mathcal{C}_f \ : \ X^3 - Y^3 = 0$$

$$\begin{array}{ccccc}
(4,0) & (4,1) & (4,2) & (4,3) & (4,4) \\
(3,0) & (3,1) & (3,2) & (3,3) & (3,4) \\
(2,0) & (2,1) & (2,2) & (2,3) & (2,4) \\
(1,0) & (1,1) & (1,2) & (1,3) & (1,4) \\
(0,0) & (0,1) & (0,2) & (0,3) & (0,4)
\end{array}$$

Permutation Polynomials and Curves over finite fields

Consider $f(x) = x^3 \in \mathbb{F}_5[x] \mapsto$ it is a PP since $(3, q-1) = (3, 4) = 1$

$$\mathcal{C}_f \; : \; X^3 - Y^3 = 0$$

$$\begin{array}{ccccc}
(4,0) & (4,1) & (4,2) & (4,3) & (4,4) \\
(3,0) & (3,1) & (3,2) & (3,3) & (3,4) \\
(2,0) & (2,1) & (2,2) & (2,3) & (2,4) \\
(1,0) & (1,1) & (1,2) & (1,3) & (1,4) \\
(0,0) & (0,1) & (0,2) & (0,3) & (0,4)
\end{array}$$

Theorem

$f(x) \in \mathbb{F}_q[x]$ *is PP* $\iff$ $\mathcal{C}_f : f(X) - f(Y) = 0$ *has only points* (a, a), $a \in \mathbb{F}_q$

THANK YOU

FOR YOUR ATTENTION