


Exercicio 1



Caesar / Rot13

Shifting cipher, which was used by Julius Caesar

Cipher

Description

Input (plaintext)

length: 14

Teste de Cesar

Encrypt

☒

Decrypt

Key:

-


3

+

Output (ciphertext)

length: 14

Whvwh gh Fhvdu



Caesar / Rot13

Shifting cipher, which was used by Julius Caesar

Cipher

Description

Input (plaintext)

length: 14

Teste de Cesar

Encrypt

☒

Decrypt

Key:

-

1

+

Output (ciphertext)

length: 14

Uftuf ef Dftbs

Cipher

Description

Input (plaintext)

length: 14

Teste de Cesar

Encrypt

☒

Decrypt

Key:

-

13

+

Output (ciphertext)

length: 14

grFGr qr PrFnE

Cipher

Description

Background

Security

About alphabets

Plaintext:

Teste de Vigenere

↓

Encrypted text:

Vlsoi fl Vdkguemi

Key:

chave

Key



QWE

Input



RTZ

Encoding/Decoding rounds



Encoding/Decoding input character R to E at position 0



Encoding/Decoding input character T to W at position 1



Encoding/Decoding input character Z to G at position 2



Encoded



EWG

AES Variants and Test Vectors

Number of Rounds: 10

-

+

S-Box

Permutation

Chaining:

None

CBC

ECB

Initial Vector (CBC only)

Key

00112233 44556677 8899aabb ccddeeff

Expanded Key

00112233 44556677 8899aabb ccddeeff c0393478 846c520f 0cf5f8b4 c028164b f67e87c2 7212d5cd 7ee72d79 becf3b32 789ca46c 0a8e71a1 74695cd8 caa667ea 54192318 5e9752b9 2afe0e61 e058698b 2ee01ef9 70774c40 5a894221 bad12baa 3011b20d 4066fe4d 1aefbc6c a03e97c6 c29906ed 82fff8a0 981044cc 382ed30a 73ff61ea f100994a 6910dd86 513e0e8c da54053b 2b549c71 424441f7 137a4f7b 36d02446 1d84b837 5fc0f9c0 4cbab6bb

Input

00000101 03030707 0f0f1f1f 3f3f7f7f

Encoding Rounds

Encoded

51bb2d07 02fec956 1e9a09e0 ec2c3875

Decoding Rounds

Decoded

00000101 03030707 0f0f1f1f 3f3f7f7f

Primes

The security of RSA is based on the fact that it is easy to calculate the product n of two large primes p and q . However, it is very difficult to determine only from the product n the two primes that yield the product. This decomposition is also called the factorization of n .

As a starting point for RSA choose two primes p and q .

1st prime p =

1373

2nd prime q =

13

For the algorithm to work, the two primes must be different.

Public key

The product n is also called modulus in the RSA method.

$$n = p \times q = 17849 \text{ (15 bit)}$$

For demonstration we start with small primes. To make the factorization difficult, the primes must be much larger. Currently, values of n with several thousand binary digits are used for secure communication.

The public key consists of the modulus n and an exponent e .

e =

7853

This e may even be pre-selected and the same for all participants.

Messages

In the following two text boxes 'Plaintext' and 'Ciphertext', you can see how encryption and decryption work for concrete inputs (numbers).

Plaintext (enter text)

Hello World

Plaintext (enter numbers, e.g. 6, 13, 111)

72,101,108,108,111,32,87,111,114,108,100



Ciphertext (enter numbers, e.g. 128, 52, 67)

17379, 11158, 10046, 10046, 10294, 5319, 484, 10294, 2981, 10046, 9415



Password Meter

Evaluates the strength of an entered password locally

How secure your password is classified by different evaluation methods, you can check here purely locally. Your entries are neither transferred nor stored. For a good password, the length is most important.

Inf0998Microsoft!

☒ Show password

☐ Manage dictionaries

Length: 17

Rating



The color of the progress bar indicates the password strength: red = very weak, yellow = medium and green = very strong.

Details

Details via zxcvbn

Time to crack (online): centuries

Time to crack (offline): 3 years

Sequences found: Inf0998 Microsoft !

Notice: -

Suggestions for improvement: -

When estimating the online cracktime, it is assumed that an attacker has no access restrictions, the server responds immediately and does not wait even after a certain number of attempts.

For offline cracktime, we assume that the attacker uses a fast PC and knows the password hash, and that the passwords have been hashed using a slow hashing method. If a fast hashing method was used instead, the time required will be significantly shorter.

Average cracktime:centuries

Sequences found:

| Pattern | Entropy | Type |
|---------|---------|----------|
| ! | 5.09 | keyboard |
| ft | 6.89 | keyboard |
| o | 4.70 | keyboard |
| s | 4.70 | keyboard |
| r | 4.70 | keyboard |
| c | 4.70 | keyboard |
| i | 4.70 | keyboard |
| M | 4.70 | keyboard |
| 0998 | 7.71 | keyboard |
| f | 4.70 | keyboard |
| n | 4.70 | keyboard |
| l | 4.70 | keyboard |








Test Your Password









Password:

Hide: ☐





Score: 100%

Complexity: Very Strong

| Additions | Rate | Count | Bonus |
|--|--------------|-------|-------|
|  Number of characters | $+(n*4)$ | 10 | + 40 |
|  Uppercase letters | $+(len-n)*2$ | 1 | + 18 |
|  Lowercase letters | $+(len-n)*2$ | 4 | + 12 |
|  Numbers | $+(n*4)$ | 4 | + 16 |
|  Symbols | $+(n*6)$ | 1 | + 6 |
|  Middle numbers or symbols | $+(n*2)$ | 4 | + 8 |
|  Requirements | $+(n*2)$ | 5 | + 10 |

| Deductions | Rate | Count | Bonus |
|---|----------|-------|-------|
|  Letters only | $-n$ | 0 | 0 |
|  Numbers only | $-n$ | 0 | 0 |
|  Repeat characters (case insensitive) | $-(n*3)$ | 3 | - 9 |
|  Consecutive uppercase letters | $-(n*2)$ | 0 | 0 |
|  Consecutive lowercase letters | $-(n*2)$ | 0 | 0 |
|  Consecutive Numbers | $-(n*2)$ | 0 | 0 |
|  Sequential letters (at least 3) | $-(n*3)$ | 0 | 0 |
|  Sequential numbers (at least 3) | $-(n*3)$ | 0 | 0 |

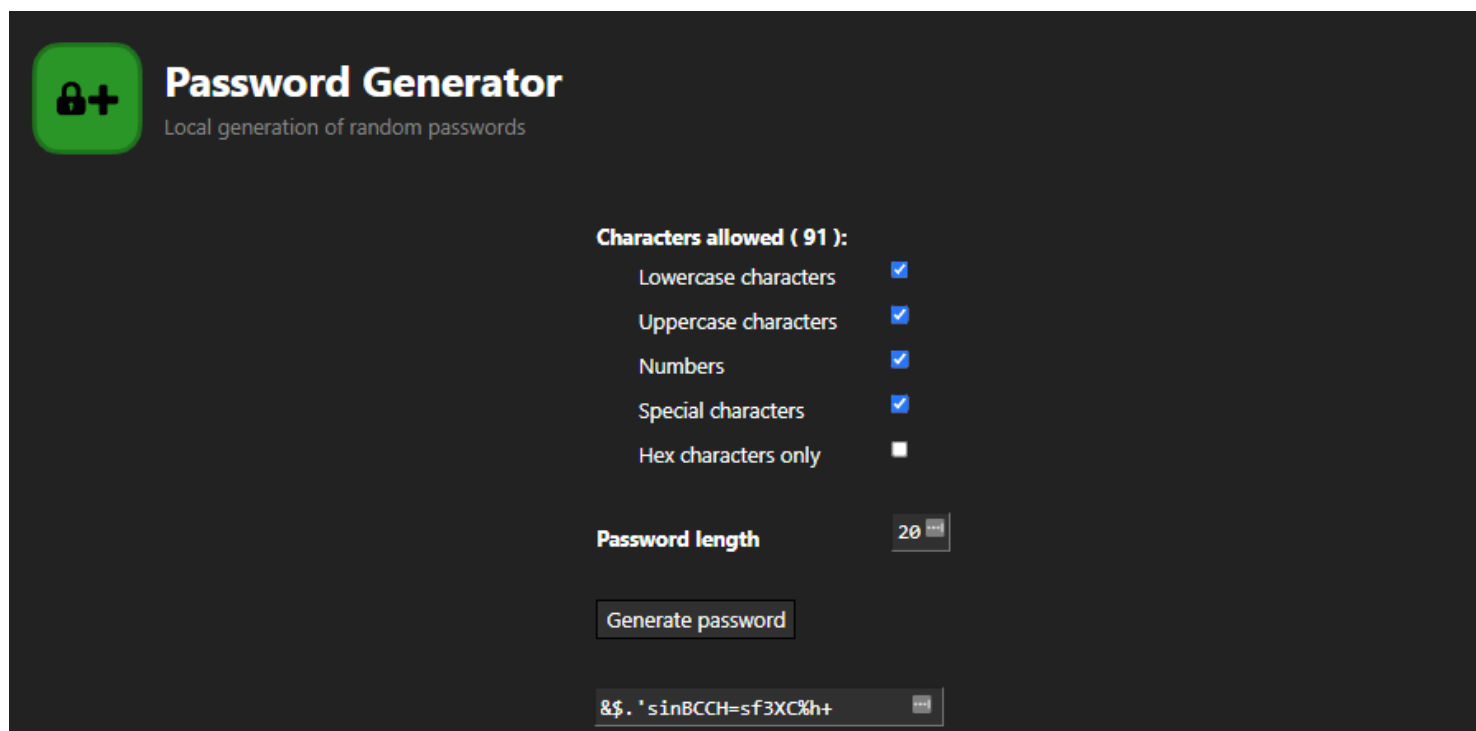
Legend

-  **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
-  **Sufficient:** Meets minimum standards. Additional bonuses are applied.
-  **Warning:** Advisory against employing bad practices. Overall score is reduced.
-  **Failure:** Does not meet the minimum standards. Overall score is reduced.

Password can only be 40 characters long.

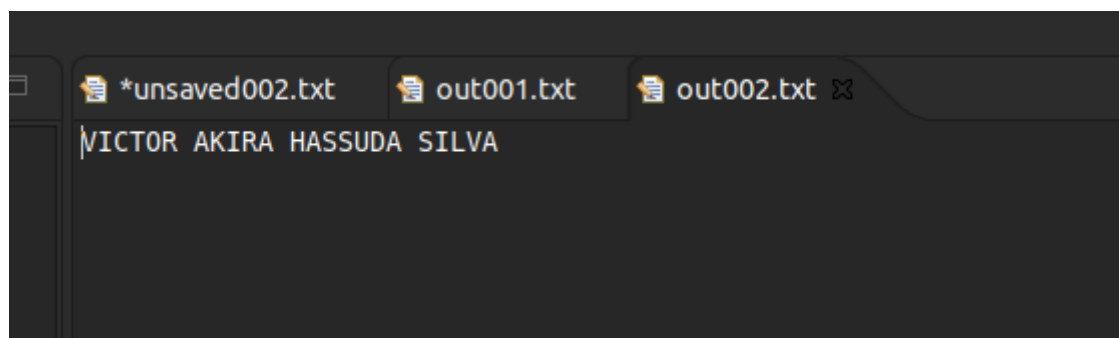
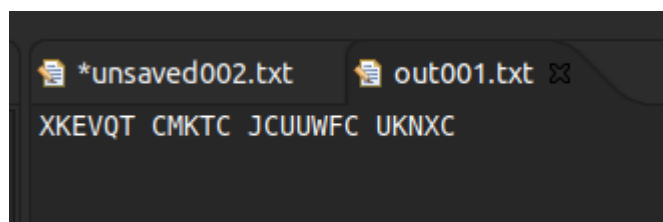
Minimum Requirements:

- Minimum 8 characters in length
- Contains 3/4 of the following characters:
 - Uppercase letters
 - Lowercase letters
 - Numbers
 - Symbols

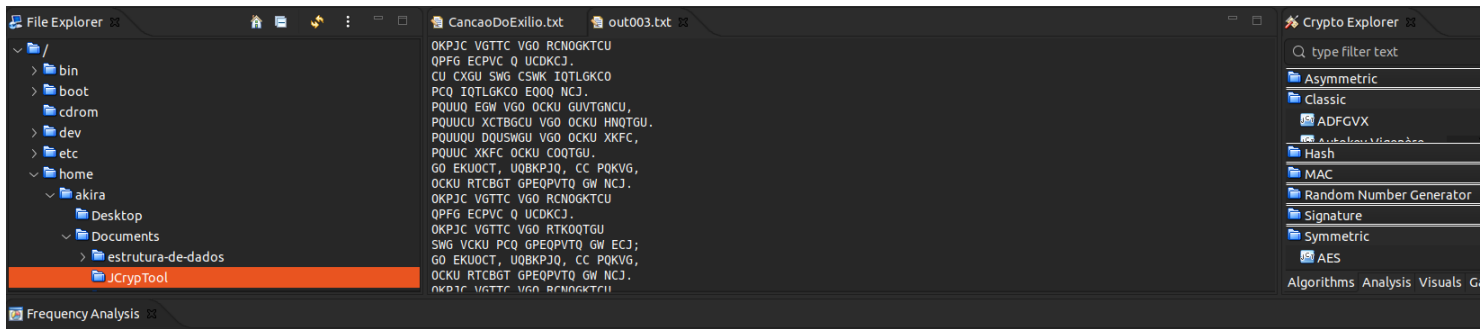
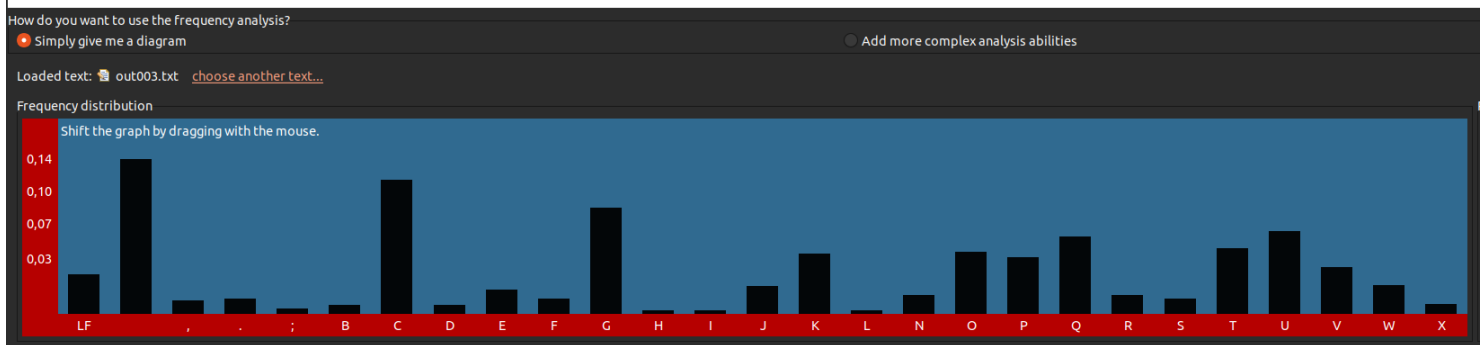
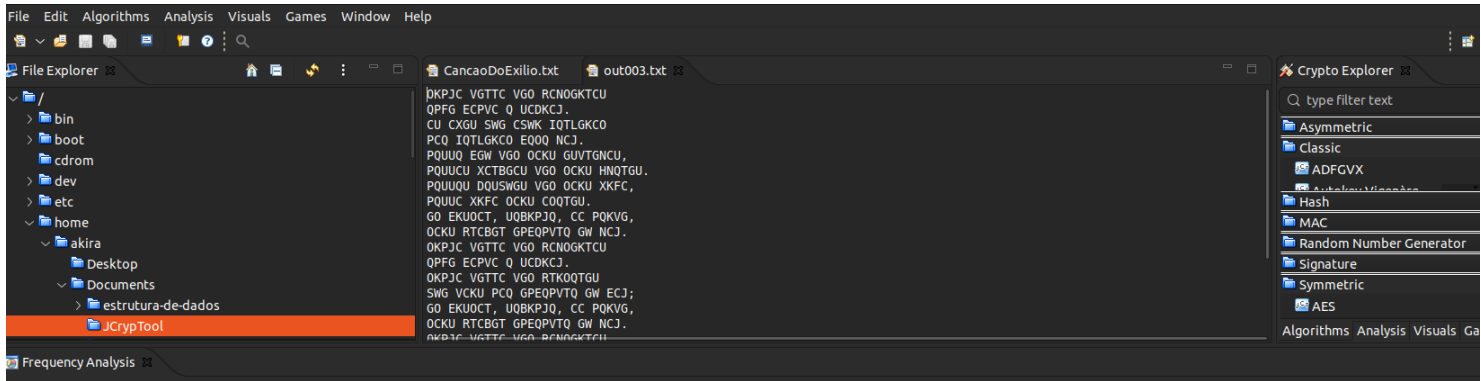


Exercicio 2

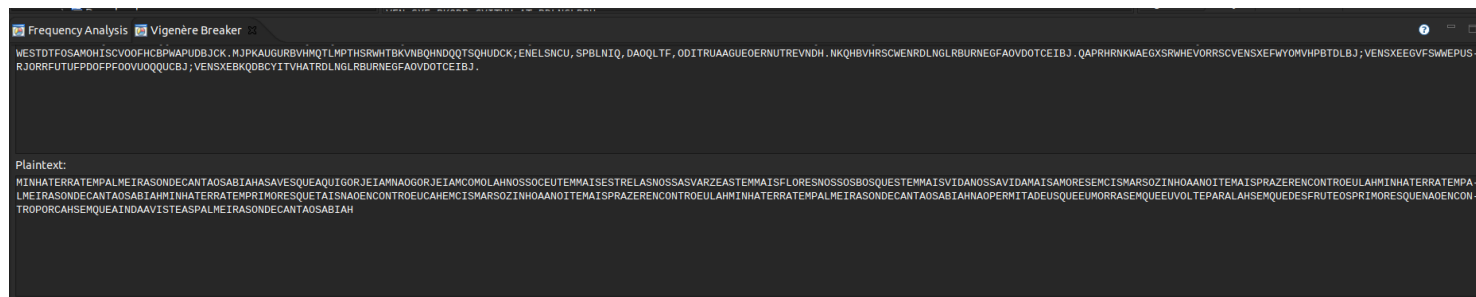
Cesar



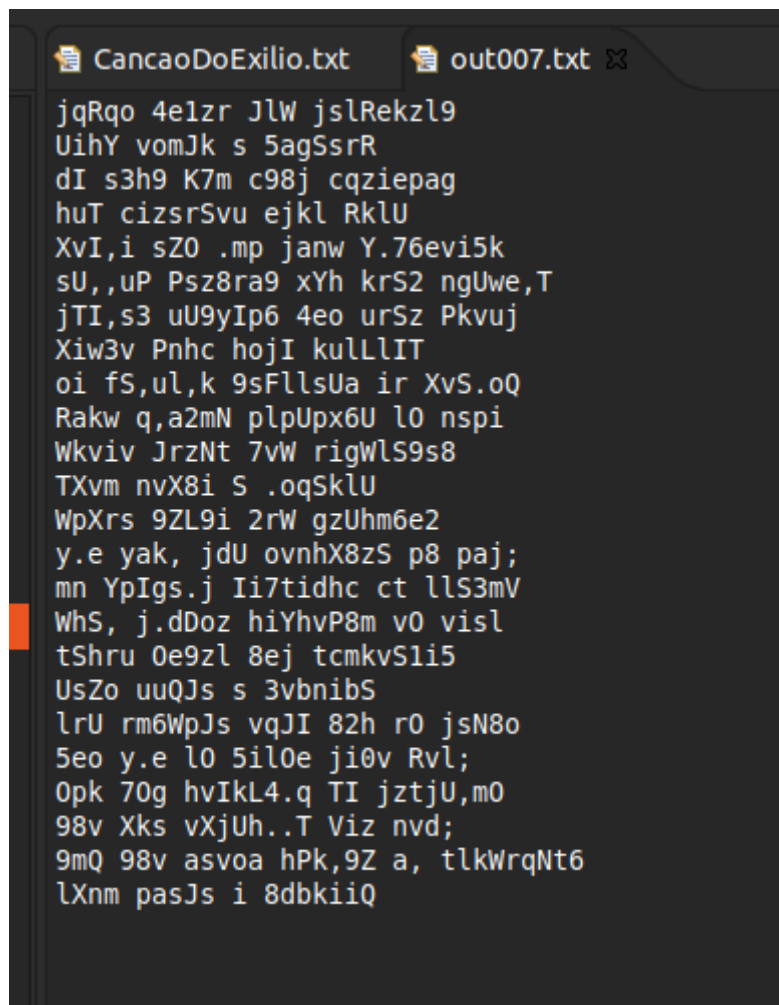
Vigenere



Após os espaços em branco, a letra 'a' é a mais frequente



XOR



```
CancaoDoExilio.txt  out007.txt  out008.txt ✕
MINHA TERRA TEM PALMEIRAS
ONDE CANTA O SABIAH.
AS AVES QUE AQUI GORJEIAM
NAO GORJEIAM COMO LAH.
NOSSO CEU TEM MAIS ESTRELAS,
NOSSAS VARZEAS TEM MAIS FLORES.
NOSSOS BOSQUES TEM MAIS VIDA,
NOSSA VIDA MAIS AMORES.
EM CISMAR, SOZINHO, AA NOITE,
MAIS PRAZER ENCONTRO EU LAH.
MINHA TERRA TEM PALMEIRAS
ONDE CANTA O SABIAH.
MINHA TERRA TEM PRIMORES
QUE TAIS NAO ENCONTRO EU CAH;
EM CISMAR, SOZINHO, AA NOITE,
MAIS PRAZER ENCONTRO EU LAH.
MINHA TERRA TEM PALMEIRAS
ONDE CANTA O SABIAH.
NAO PERMITA DEUS QUE EU MORRA
SEM QUE EU VOLTE PARA LAH;
SEM QUE DESFRUTE OS PRIMORES
QUE NAO ENCONTRO POR CAH;
SEM QUE AINDA AVISTE AS PALMEIRAS
ONDE CANTA O SABIAH.|
```

RC6

```
16blocoستextoclaro.txt  out009.bin  out010.bin  out011.bin ✕
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE .....U..-.....
018: D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .U..-.....U..-...
030: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE .....U..-.....
048: D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .U..-.....U..-...
060: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE .....U..-.....
078: D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .U..-.....U..-...
090: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE .....U..-.....
0A8: D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .U..-.....U..-...
0C0: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE .....U..-.....
0D8: D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .U..-.....U..-...
0F0: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .....U..-...
108:
```

```
16bloco textoclaro.txt out009.bin out010.bin out011.bin *out012.bin out014.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF01234567
018: 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 89ABCDEF0123456789ABCDEF
030: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF01234567
048: 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 89ABCDEF0123456789ABCDEF
060: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF01234567
078: 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 89ABCDEF0123456789ABCDEF
090: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF01234567
0A8: 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 89ABCDEF0123456789ABCDEF
0C0: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF01234567
0D8: 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 89ABCDEF0123456789ABCDEF
0F0: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF
108:
120:
138:
```

```
16bloco textoclaro.txt out009.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE .....U.....
018: D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .U.....U....
030: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE .....U.....
048: D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .U.....U.....
060: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE .....U.....
078: D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .U.....U.....
090: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE .....U.....
0A8: D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .U.....U.....
0C0: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE .....U.....
0D8: D7 55 02 95 2D 98 F1 8C 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C .U.....U.....
0F0: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 20 08 28 28 CE 91 49 A2 .....U.....((..I.
108: 72 AE D7 D9 2F 6A 86 8D ..... r.../j...
120:
138:
150:
168:
```

```
16bloco textoclaro.txt out009.bin out010.bin out011.bin *out012.bin out014.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF01234567
018: 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 89ABCDEF0123456789ABCDEF
030: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF01234567
048: 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 89ABCDEF0123456789ABCDEF
060: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF01234567
078: 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 89ABCDEF0123456789ABCDEF
090: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF01234567
0A8: 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 89ABCDEF0123456789ABCDEF
0C0: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 0123456789ABCDEF01234567
0D8: 38 39 41 42 43 44 45 46 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 89ABCDEF0123456789ABCDEF
0F0: 30 31 32 33 34 35 36 37 38 39 41 42 43 44 45 46 10 10 10 10 10 10 10 10 0123456789ABCDEF.....
108: 10 10 10 10 10 10 10 10 .....
120:
138:
150:
```

CBC

```
16bloco textoclaro.txt out015.bin out016.bin out017.bin out018.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 2E D0 FC 9D B7 14 9F FE D7 55 02 95 2D 98 F1 8C 20 1C 22 FD 41 E4 EC 06 .....U...-... ".A...
018: BB 5E 71 3A 5B 6B 53 84 3E 2F 09 91 6F 34 3F FA 9C 8C FF 80 58 A3 B0 79 .^q:[kS.>/..o4?...X..y
030: 4A 83 51 E9 65 2C A2 38 AD B1 54 F5 E5 22 53 E5 85 8D 86 05 55 FE 46 25 J.Q.e,.8..T.."S.....U.F%
048: 28 F3 A5 BD 82 45 00 D8 1A AF FF 6C CE 53 69 3A 81 8C 64 1D 23 E5 04 E5 (...E.....l.Si:..d.#...
060: EE 15 A0 EF 02 0A A5 39 CF 7D 83 A7 38 8D B2 2E 97 1B E0 8E 01 29 CA C1 .....9.}.8.....)..
078: 4C A2 EB CB 78 8D C5 7A 0D 26 FE 86 3F 20 1B 09 EA CF ED 09 86 EE D5 3B L...x..z.&..? .....;
090: 04 F9 CD FB 31 DE 2E 43 CC EE 4E 6F 76 B5 36 20 51 C4 6A 14 E4 BD D4 5A ....1..C..Nov.6 Q.j....Z
0A8: 87 25 98 FA EA 29 89 A3 24 C9 CC 3B 6E 26 1C A6 01 30 7C AC 7E 64 82 8F .%....)..$.;n&...0|.~d..
0C0: BA B2 85 89 C6 A4 60 24 A9 3E 6B F5 86 4A B1 85 A7 06 52 F7 FF 86 1B 55 .....`$.>k..J.....R....U
0D8: C3 CF 06 1D 77 C9 4B B3 24 DF 0A 7F EB 45 0F 80 27 42 1F 8E BC C8 12 FF .....w.K.$....E..'B.....
0F0: 62 15 52 5D FC 22 AE 48 04 EA 08 33 62 83 93 A5 3A 0F F1 DA 79 90 00 03 b.R].."H...3b....y...
108: C1 2C 83 CC 18 2C 18 34 .....4 .....
120:
138:
150:
```

CFB

```
16bloco textoclaro.txt out015.bin out016.bin out017.bin out018.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 55 B7 9C 94 5E 9A A6 59 08 75 E6 66 F9 6F 5E A6 CA 96 F9 05 F1 9D 8F C7 U...^..Y.u.f.o^.....
018: CF 1A 76 D3 DA D4 B9 3E AF B2 1D E9 14 47 10 68 3A EE 22 2B DE 5D 2D 77 ..v....>.....G.h:."+.]~w
030: B2 BA 6F CC 9C 7F 73 07 D2 71 46 95 73 30 93 6F 95 89 7A 64 69 75 7E AA ..o....qF.s0.o..zdiu~.
048: 93 8E 45 2C 6D 9B D0 27 2C 6B 5B B1 82 6E 9E 97 68 3F 04 FE 53 06 E2 75 ..E,m..',k[.n..h?...S..u
060: 87 F3 91 C1 D4 76 2E 3B CF 29 7C 62 4D D6 BD 6D 00 C7 03 EF E6 BC 02 5B ....v.;.)|bM..m.....[
078: 2F 9F 02 92 12 65 57 3B 01 8A A0 93 1F F8 82 E1 95 C4 5D 1C 94 F4 47 7D /....eW;.....]...G}
090: 46 4D 91 A8 30 45 2F 41 59 BB 87 B1 3D 77 2B 00 D3 88 3B 8F 20 1E 50 74 FM..0E/AY...=w+...;. .Pt
0A8: 37 09 21 EF 61 4C 7C 02 25 F5 8A 16 12 03 9F 84 DD B0 FB 20 72 30 36 04 7.!.aL|.%...... r06.
0C0: 49 A5 E0 85 00 72 A3 7E 6D 18 4D 1A EF D2 5B 22 4F CE 0A 34 DA 29 D2 CB I....r..~m.M...["0..4.)..
0D8: 9D 19 BF 2D F7 49 93 C8 A6 D1 3F 51 A8 CB AD BE 6A CA 85 A3 C0 0E 3A A7 ....-I....?Q....j.....:
0F0: 25 F4 11 C1 FD 28 0E 2C C8 DF F3 9C F3 DE 49 D8 67 98 67 78 9A 14 C1 8E %....(,.....I.g.gx....
108: 16 90 2E 25 8B B8 09 34 .....4 .....
120:
138:
```

OFB

```
16bloco textoclaro.txt out015.bin out016.bin out017.bin out018.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 55 B7 9C 94 5E 9A A6 59 08 75 E6 66 F9 6F 5E A6 B5 16 83 59 61 1A FA 98 U...^..Y.u.f.o^....Ya...
018: A8 D2 83 BC 03 29 B8 7D EB F8 9B 93 FA 18 E9 F0 A5 95 99 5B 92 77 A4 11 .....).}.....[.w..
030: 8B 01 88 A8 2F 7B 5E E9 4D 72 3D B9 A1 C5 30 40 D5 52 35 8C B7 F3 6A 89 ..../{^..Mr=...0@..R5...j.
048: A5 DD 65 EE D0 92 E9 38 22 54 DF 1D 6C 57 5E 7E 8A 63 30 07 D3 AA 13 36 ..e....8"T..lW^~.c0....6
060: 43 BE DA B8 D1 96 74 B1 00 24 AB EC EF AB 55 26 96 A1 91 A6 C4 8D AF 4C C....t...$.U&.....L
078: 1F 70 60 C9 3C 96 9C 5B 62 E6 6D 20 34 81 E5 89 2F C7 5F BE FF 91 A1 BE .p`.<..[b.m 4.../_.....
090: 14 F6 5C E1 78 31 BF 08 89 43 B9 FE 4C 0B 4A 94 E0 B2 06 7B A3 06 CB 47 ...\.x1...C..L.J....{...G
0A8: DC 52 5E AF 91 9A 41 D9 96 79 B8 C8 CF BD 30 43 6E 0D 2B C2 6B 00 0D 7B .R^...A..y....0Cn.+k...{
0C0: EB 1C DC 81 08 59 45 E6 B2 D6 1E EC FB CE E1 5F 76 07 D9 D6 DE D5 68 DE .....YE.....v.....h.
0D8: 55 41 78 85 F3 08 41 D3 8B 2E 0F E4 D6 16 F2 C6 A6 C4 7B FB 60 AB 75 19 UAx...A.....{..`..u.
0F0: 1F 70 50 3C D9 46 47 B4 63 FE BD D5 A7 BD E9 B7 B5 9E F4 09 9B E9 60 9A .pP<.FG.c.....`..
108: D7 DA 3A 3C 8E 1B 0F 81 .....<.....
120:
138:
```

CTR


```
16bloco texto claro.txt  out015.bin  out016.bin  out017.bin  out018.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 55 B7 9C 94 5E 9A A6 59 08 75 E6 66 F9 6F 5E A6 2A 23 FE C7 B9 85 A7 10 U...^..Y.u.f.o^.*#.....
018: 37 32 6B E9 49 6C EA 70 D1 7C 94 29 3F 36 D1 3C EE FC 28 99 64 A6 9C A8 72k.Il.p.|.)?6.<..(.d...
030: 0D FC DC 95 A9 CD 62 84 59 12 39 6E 92 4A 76 2A 37 7E 2B 7C 90 FA 32 BF .....b.Y.9n.Jv*7~+|..2.
048: 78 64 0B 81 30 5E 64 3C 78 A7 63 D6 05 DC 29 0E 86 AA 2A 33 41 BA FF 63 xd..0^d<x.c...)...*3A..c
060: 8F 06 5A FF B7 E5 3D 15 AE BF CD 5A F0 27 4F 52 D0 D6 AA 97 E2 98 3F 9A ..Z...=....Z.'OR.....?.
078: AA 1A 78 C3 D9 FD BA 1A 1C 1C 80 68 E9 D6 AF 81 7E E1 D5 3B 61 AE D7 43 ..x.....h.....~...;a..C
090: BE FE ED AB 87 6B A4 65 92 3C B7 E4 7D 66 4E 41 60 2F CB 41 05 BE 99 0F .....k.e.<...}fNA`/.A....
0A8: 5F F0 43 1E 9E B6 1C C4 31 DA FB 57 EE E1 10 62 06 1A DF 9F F7 FA FC A7 _..C.....1..W...b.....
0C0: F2 B7 82 44 1A 06 0A DF 76 3E 71 5E FB 7B 9B 76 24 B6 C2 4F FF 8B 12 5C ...D....v>q^.{.v$.0...\
0D8: D4 39 92 86 63 78 BC 0D 8D 19 56 69 31 A6 66 92 F9 D4 D6 AB 75 47 CB 5B .9..cx....Vi1.f.....uG.[
0F0: 27 92 6A A4 39 EB 4F 63 25 D9 62 15 65 98 3C DA B4 23 7C 90 9A 09 78 46 '.j.9.0c%.b.e.<..#|...xF
108: 94 40 FE 31 57 C1 B0 25 .....@.1W..%
120:
```

ARC4

```
CancaoDoExilio.txt  out019.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: C8 32 C2 3F F3 07 15 E0 8A 2B D8 1B E1 20 10 B4 79 A4 FF 3D C4 7E F9 4F .2.?.....+... ..y..=..~.0
018: 13 AB 44 10 35 98 C7 7E 22 F5 C1 C8 26 4F B2 59 D0 15 F1 23 45 49 76 BF ..D.5..~"...&0.Y...#Eiv.
030: 27 01 01 7D 26 CB 88 C9 D4 1A 70 C0 C0 F2 77 E0 75 9C D0 39 33 3B E8 AB '...}&.....p...w.u..93;..
048: 0D BB 11 CF 17 B8 AA 7F 5B 66 A6 96 20 C2 15 0D 0D C4 B8 B5 35 B7 CD 1F .....[f... ..5....
060: 00 40 6F 7B 71 31 A4 11 BA D6 03 E6 7F F6 ED 30 F9 0D 5C 96 54 78 65 38 .@o{q1.....0...\Txe8
078: 9E FA 0B B7 BE 06 B7 F6 F7 EE 7F 28 65 FA 3C 4B 96 F1 FB CA 02 50 58 7A .....(e.<K...PXz
090: 98 E5 EC F8 13 14 7E 4F 48 C9 3A 52 6B E7 F3 48 C1 7D C0 FB 79 CF 00 95 .....~0H.:Rk..H.}.y...
0A8: E5 67 FE 2F 2C BD 12 D7 2F 43 66 F9 B8 82 AA D0 CD D1 B8 65 3C AD C6 5F .g./,.../Cf.....e<..._
0C0: 7B 51 AE 89 DA 7E C6 E2 44 CF CD 1D 2B AF C1 09 DA 7D 94 17 D2 6F E9 A6 {Q...~..D...+....}...o..
0D8: A7 80 62 87 55 80 37 7A 77 4B C5 F7 F3 88 76 A1 76 05 50 7B 06 88 0B B6 ..b.U.7zwK....v.v.P{....
0F0: 78 0F 5C 58 7E B2 EF C1 DD 4B E5 AF 48 66 73 61 28 91 7B B7 CC 0A F8 AE x.\X~....K..Hfsa(.{.....
108: 01 16 46 C5 D8 8C 2A F4 6B EF 14 E1 C6 0C 97 56 A0 9C 7D 83 C1 95 08 10 ..F...*.k.....V..}....
120: 97 37 11 5B 41 DF 9C 1D 18 73 3D E8 C1 97 35 52 6D 6B E1 7F 12 AF D7 4A .7.[A....s=...5Rmk.....J
138: C7 FA 6B BE 14 89 95 01 23 B2 4E A9 AD D2 5D 3D AD 92 1B 67 B5 C1 6B 71 ..k.....#.N...]=...g..kq
150: 1F D3 9A A7 10 BA D0 70 75 B2 DE C3 53 1F 2E 02 F9 A9 13 7D CD 2D 6A 0B .....pu...S.....}.-j.
168: 1E C2 B7 0D F9 9F 1B 3A 82 1A BB 24 FE F2 C6 E1 DB 94 FF F7 F4 F0 98 5D .....:...$......]
180: 21 30 30 9F 1C 12 17 67 2B 92 2D A0 F8 8E A6 F2 CB 5B 25 9A 18 8E 5C 31 !00....g+.-.....[%..\1
198: A4 DC 83 C2 56 B9 BF B2 B2 4D 72 FF 43 2B AD 74 B2 6A 89 19 63 F0 DC 4A ....V....Mr.C+.t.j..c...J
1B0: DF A0 94 1F 86 89 FC C9 68 E3 B3 93 65 2A 44 87 98 C9 05 30 BB B7 20 A8 .....h....e*D....0...
1C8: 46 79 23 01 AE A9 AC E2 A4 8E 11 09 87 5D E5 67 25 6A 18 3E A8 0E 62 CC Fy#.....].g%j.>..b.
1E0: 6A 58 3F 30 90 26 72 6E D5 DB 10 5F 53 F7 C4 BF 1D 03 6B A4 9A B0 61 8D jX?0.&rn..._S.....k...a.
1F8: 44 08 9D CF 4A C6 3F B6 1E 02 C1 CC FC 2E 48 C4 8A DD D3 4B 49 56 11 64 D...J.?.....H....KIV.d
210: 2A DD B0 12 7E E6 AC 86 DD 88 FF F6 9D 80 3A F6 C0 06 AA 8E 7D 69 41 4C *...~.....:.....}iAL
228: 9E C4 5C 13 A9 EE 24 EA 3C 21 5F 3B 1A E4 9A 70 8C A0 A7 78 D2 56 D4 79 ..\...$.<!_;...p...x.V.y
240: 62 FA 4E CD B1 24 28 E3 2F DE AB E5 9F AC 37 11 AB B0 09 79 A2 0D 3B C6 b.N...$(!/.....7....y...;
258: 7D F3 0C FE BE BD B9 B8 CC 16 1A B7 AC 1B 69 2A B4 34 05 94 59 EC 08 E8 }.....i*.4..Y...
270: A7 24 16 BB FA A0 22 DD 24 FB FD 8F 3B 6C 50 78 A8 7C 8A 8C .....$.....".$....;lPx.|..
288:
2A0:
```

```
CancaoDoExilio.txt out019.bin out020.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 4D 69 6E 68 61 20 74 65 72 72 61 20 74 65 6D 20 70 61 6C 6D 65 69 72 61 Minha terra tem palmeira
018: 73 0A 4F 6E 64 65 20 63 61 6E 74 61 20 6F 20 73 61 62 69 61 68 2E 0A 41 s.Onde canta o sabiah..A
030: 73 20 61 76 65 73 20 71 75 65 20 61 71 75 69 20 67 6F 72 6A 65 69 61 6D s aves que aqui gorjeiam
048: 0A 4E 61 6F 20 67 6F 72 6A 65 69 61 6D 20 63 6F 6D 6F 20 6C 61 68 2E 0A .Nao gorjeiam como lah..
060: 4E 6F 73 73 6F 20 63 65 75 20 74 65 6D 20 6D 61 69 73 20 65 73 74 72 65 Nosso ceu tem mais estre
078: 6C 61 73 2C 0A 4E 6F 73 73 61 73 20 76 61 72 7A 65 61 73 20 74 65 6D 20 las,.Nossas varzeas tem
090: 6D 61 69 73 20 66 6C 6F 72 65 73 2E 0A 4E 6F 73 73 6F 73 20 62 6F 73 71 mais flores..Nossos bosq
0A8: 75 65 73 20 74 65 6D 20 6D 61 69 73 20 76 69 64 61 2C 0A 4E 6F 73 73 61 ues tem mais vida,.Nossa
0C0: 20 76 69 64 61 20 6D 61 69 73 20 61 6D 6F 72 65 73 2E 0A 45 6D 20 63 69 vida mais amores..Em ci
0D8: 73 6D 61 72 2C 20 73 6F 7A 69 6E 68 6F 2C 20 61 61 20 6E 6F 69 74 65 2C smar, sozinho, aa noite,
0F0: 0A 4D 61 69 73 20 70 72 61 7A 65 72 20 65 6E 63 6F 6E 74 72 6F 20 65 75 .Mais prazer encontro eu
108: 20 6C 61 68 2E 0A 4D 69 6E 68 61 20 74 65 72 72 61 20 74 65 6D 20 70 61 lah..Minha terra tem pa
120: 6C 6D 65 69 72 61 73 0A 4F 6E 64 65 20 63 61 6E 74 61 20 6F 20 73 61 62 lmeiras.Onde canta o sab
138: 69 61 68 2E 0A 4D 69 6E 68 61 20 74 65 72 72 61 20 74 65 6D 20 70 72 69 iah..Minha terra tem pri
150: 6D 6F 72 65 73 0A 51 75 65 20 74 61 69 73 20 6E 61 6F 20 65 6E 63 6F 6E mores.Que tais nao encon
168: 74 72 6F 20 65 75 20 63 61 68 3B 0A 45 6D 20 63 69 73 6D 61 72 2C 20 73 tro eu cah;.Em cismar, s
180: 6F 7A 69 6E 68 6F 2C 20 61 61 20 6E 6F 69 74 65 2C 0A 4D 61 69 73 20 70 ozinho, aa noite,.Mais p
198: 72 61 7A 65 72 20 65 6E 63 6F 6E 74 72 6F 20 65 75 20 6C 61 68 2E 0A 4D razer encontro eu lah..M
1B0: 69 6E 68 61 20 74 65 72 72 61 20 74 65 6D 20 70 61 6C 6D 65 69 72 61 73 inha terra tem palmeiras
1C8: 0A 4F 6E 64 65 20 63 61 6E 74 61 20 6F 20 73 61 62 69 61 68 2E 0A 4E 61 .Onde canta o sabiah..Na
1E0: 6F 20 70 65 72 6D 69 74 61 20 44 65 75 73 20 71 75 65 20 65 75 20 6D 6F o permita Deus que eu mo
1F8: 72 61 0A 53 65 6D 20 71 75 65 20 65 75 20 76 6F 6C 74 65 20 70 61 72 rra.Sem que eu volte par
210: 61 20 6C 61 68 3B 0A 53 65 6D 20 71 75 65 20 64 65 73 66 72 75 74 65 20 a lah;.Sem que desfrute
228: 6F 73 20 70 72 69 6D 6F 72 65 73 0A 51 75 65 20 6E 61 6F 20 65 6E 63 6F os primores.Que nao enco
240: 6E 74 72 6F 20 70 6F 72 20 63 61 68 3B 0A 53 65 6D 20 71 75 65 20 61 69 ntro por cah;.Sem que ai
258: 6E 64 61 20 61 76 69 73 74 65 20 61 73 20 70 61 6C 6D 65 69 72 61 73 0A nda aviste as palmeiras.
270: 4F 6E 64 65 20 63 61 6E 74 61 20 6F 20 73 61 62 69 61 68 2E Onde canta o sabiah.
```

AES ECB

```
CancaoDoExilio.txt out021.bin out024.bin out025.bin out026.bin out027.bin out028.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
000: 77 E6 D1 5D F7 04 1A 1 D6 14 23 CF DF 21 B1 4 E1 06 9D 84 92 B5 FD 8 60 A9 AA 50 39 88 16 .w..]...A..#..!.....P9..
020: D C8 28 08 05 2C 4D A0 C 21 40 1A 69 72 7B B1 2 D8 E5 CC D1 52 32 63 8 2F 64 A5 D3 04 48 C6 =.(.,M..!@.ir{.2....R2c./d...H.
040: 6 55 FD 76 C9 1C 8D B0 9 32 CD EB 97 61 A4 C5 7 56 38 75 B4 E1 66 8E D 65 A1 A6 33 58 36 9C .U.v.....2...a...V;u..f.=e..3X6.
060: 6 BE DE 0C 9C 44 7A A8 5 4A 84 15 7F E8 B8 21 9 83 86 FD 8C 5C CF 21 F C1 DB 29 32 8C 26 2D .....Dz.uJ.....!.....\.....)2.&-
080: 9 C3 17 BD 30 2F 13 2D 3 37 C3 8B 8D FD 86 61 E 84 15 C2 76 F5 DC 73 4 78 F6 C9 BE 10 51 38 ....0/-..7.....a....v..s${....Q8
0A0: 8 FE 9C 39 53 5E 83 07 7 42 FD 6C 9E C8 8B 68 9 EF 1C D8 4E 71 20 92 5 C2 EC 43 FD 27 51 C9 ...9S^...B.l...h9...Nq ....C.'Q.
0C0: 4 8B 2E 7F 2E 88 BC 22 E C6 19 5B 90 3C 20 46 4 4C E5 3F E0 A1 23 4E D 88 2F 82 7C 03 7E AC .....".[.< F.L.?..#N=../.]~.
0E0: B C5 C8 B9 F0 61 5B A7 7 45 49 25 0B 90 D4 FC B 90 E0 45 B3 09 98 03 2 A7 B9 E8 B9 2E 68 C5 {...a[gEI%.....E.....h.
100: C E4 62 4D 42 4A E9 77 B 20 12 90 E9 84 8C 11 D CE D2 3B 5C E1 07 A2 D EB 4B C7 F0 6E 74 B9 ..bMBJ.w. ....;...\...=..K..nt.
120: 9 49 BD F3 B8 42 77 02 B 2D 56 94 CF 69 2D 54 A E5 83 9C F4 75 D0 C0 9 50 A8 16 FD 84 E7 8D yI...Bw...-V..i-T.....u..yP.....
140: 6 38 24 25 DB 22 31 7B F DD 70 C5 E5 1B A6 F8 E 8C 2A 82 FC 90 60 D7 B 56 99 08 FD 71 B0 B0 &8$%."i{..p.....>.*....V...q..
160: 0 00 0E B6 BB EF 32 EA E DB C1 C4 84 EF 49 2F 1 0F 8A E3 40 E8 E0 CD 1 E8 D8 73 58 67 B6 34 P.....2.....I/....@...a..sXg.4
180: F 6B 2A 2E E5 AB F7 A5 3 AB AA 8E 0B 8B 3A 01 7 2B A4 59 E6 9F 42 6E B B2 7B 55 8E 92 15 19 _k*.....:..w+.Y..Bn...{U....
1A0: 3 3F EA 31 3B 0F E6 F4 B 04 40 CF A5 A8 78 DF 2 2A 44 EC 4C 78 50 79 C 4C A6 56 AB 2B 41 29 .?.1;...+@...x..."D.LxPy.L.V.+A)
1C0: 9 20 CF 82 13 DB 73 EC 9 E0 81 13 8C 94 4A D8 6 21 B9 6A AE 1C 4D AE F 55 17 0D BF 69 28 46 . ....s.....J.F!.j..M...U...i(F
1E0: C F6 A6 9D AD 33 10 92 7 4A 90 0E 44 40 D2 CA 9 79 25 E8 19 5F 54 0A 8 A8 1F 05 E4 44 81 CF .....3...J..D@...y%..._T.....D..
200: 3 39 68 18 3F D2 EE 97 B 0C 71 6A 3A 7E 37 3C D AA D1 D4 A8 47 87 63 C 53 8C A6 41 81 A3 B0 #9h.?.....qj:~7<=...G.c.S..A...
220: 2 36 26 9F 09 8F 04 31 4 8E 23 E5 5F 93 C1 72 1 51 E8 7D CF C6 AA A1 6 5D 50 8E E4 53 E2 0D r6&...1d.#..._r.Q}.....]P...S..
240: 0 55 0D 43 41 FA FB 60 1 CA 0E 8D 28 B4 50 50 C FC 36 4F 2F D8 9E DE 5 D0 18 17 29 BA B7 18 .U.CA..'. ....(.PP..60/.....)....
260: 4 16 65 22 18 2A 8B 62 9 64 8F 40 AA D2 09 53 F E7 98 0F E9 AA B7 47 5 BE B3 17 5E FC 23 AE $e".*.b.d.@...S.....G.....^.#..
280:
```



```
CancaoDoExilio.txt  out021.bin  out024.bin  out025.bin  out026.bin  out027.bin  out028.bin  x3
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F
000: 4D 69 6E 68 61 20 74 65 72 72 61 20 74 65 6D 20 70 61 6C 6D 65 69 72 61 73 0A 4F 6E 64 65 20 63 Minha terra tem palmeiras.Onde c
020: 61 6E 74 61 20 6F 20 73 61 62 69 61 68 2E 0A 41 73 20 61 76 65 73 20 71 75 65 20 61 71 75 69 20 anta o sabiah..As aves que aqui
040: 67 6F 72 6A 65 69 61 6D 0A 4E 61 6F 20 67 6F 72 6A 65 69 61 6D 20 63 6F 6D 6F 20 6C 61 68 2E 0A gorjeiam.Nao gorjeiam como lah..
060: 4E 6F 73 73 6F 20 63 65 75 20 74 65 6D 20 6D 61 69 73 20 65 73 74 72 65 6C 61 73 2C 0A 4E 6F 73 Nosso ceu tem mais estrelas..Nos
080: 73 61 73 20 76 61 72 7A 65 61 73 20 74 65 6D 20 6D 61 69 73 20 66 6C 6F 72 65 73 2E 0A 4E 6F 73 sas varzeas tem mais flores..Nos
0A0: 73 6F 73 20 62 6F 73 71 75 65 73 20 74 65 6D 20 6D 61 69 73 20 76 69 64 61 2C 0A 4E 6F 73 73 61 sos bosques tem mais vida..Nossa
0C0: 20 76 69 64 61 20 6D 61 69 73 20 61 6D 6F 72 65 73 2E 0A 45 6D 20 63 69 73 6D 61 72 2C 20 73 6F vida mais amores..Em cismar, so
0E0: 7A 69 6E 68 6F 2C 20 61 61 20 6E 6F 69 74 65 2C 0A 4D 61 69 73 20 70 72 61 7A 65 72 20 65 6E 63 zinho, aa noite..Mais prazer enc
100: 6F 6E 74 72 6F 20 65 75 20 6C 61 68 2E 0A 4D 69 6E 68 61 20 74 65 72 72 61 20 74 65 6D 20 70 61 ontro eu lah..Minha terra tem pa
120: 6C 6D 65 69 72 61 73 0A 4F 6E 64 65 20 63 61 6E 74 61 20 6F 20 73 61 62 69 61 68 2E 0A 4D 69 6E lmeiras.Onde canta o sabiah..Min
140: 68 61 20 74 65 72 72 61 20 74 65 6D 20 70 72 69 6D 6F 72 65 73 0A 51 75 65 20 74 61 69 73 20 6E ha terra tem primores.Que tais n
160: 61 6F 20 65 6E 63 6F 6E 74 72 6F 20 65 75 20 63 61 68 3B 0A 45 6D 20 63 69 73 6D 61 72 2C 20 73 ao encontro eu cah;Em cismar, s
180: 6F 7A 69 6E 68 6F 2C 20 61 61 20 6E 6F 69 74 65 2C 0A 4D 61 69 73 20 70 72 61 7A 65 72 20 65 6E ozinho, aa noite..Mais prazer en
1A0: 63 6F 6E 74 72 6F 20 65 75 20 6C 61 68 2E 0A 4D 69 6E 68 61 20 74 65 72 72 61 20 74 65 6D 20 70 contro eu lah..Minha terra tem p
1C0: 61 6C 6D 65 69 72 61 73 0A 4F 6E 64 65 20 63 61 6E 74 61 20 6F 20 73 61 62 69 61 68 2E 0A 4E 61 almeiras.Onde canta o sabiah..Na
1E0: 6F 20 70 65 72 6D 69 74 61 20 44 65 75 73 20 71 75 65 20 65 75 20 6D 6F 72 72 61 0A 53 65 6D 20 o permita Deus que eu morra.Sem
200: 71 75 65 20 65 75 20 76 6F 6C 74 65 20 70 61 72 61 20 6C 61 68 3B 0A 53 65 6D 20 71 75 65 20 64 que eu volte para lah;Sem que d
220: 65 73 66 72 75 74 65 20 6F 73 20 70 72 69 6D 6F 72 65 73 0A 51 75 65 20 6E 61 6F 20 65 6E 63 F esfrute os primores.Que nao enco
240: 6E 74 72 6F 20 70 6F 72 20 63 61 68 3B 0A 53 65 6D 20 71 75 65 20 61 69 6E 64 61 20 61 76 69 73 ntro por cah;Sem que ainda avis
260: 74 65 20 61 73 20 70 61 6C 6D 65 69 72 61 73 0A 4F 6E 64 65 20 63 61 6E 74 61 20 6F 20 73 61 te as palmeiras.Onde canta o sa
280:
2A0:
```

CBC

```
CancaoDoExilio.  out021.bin  out024.bin  x3  out026.bin  out027.bin  out028.bin  "1
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 80 77 E6 D1 5D F7 04 1A 41 D6 14 23 CF DF 21 B1 56 AE 43 3F 9F FF D3 E9 .w..]...A.#...!.V.C?....
018: D1 F4 C4 D4 06 66 F2 E2 2A 74 C4 D0 24 C6 A8 D7 35 0B B1 C3 E2 4F C6 B9 .....f...*t...$....5....0..
030: 0C 1A C1 8D FA E4 5A 1C 1B 8E 62 0D 8F 4B FD 31 7D 85 B1 B2 50 AE 3C 11 .....Z...b...K.1)...P.<.
048: FA D2 A6 03 82 7E DB C8 5E 46 C5 E7 EB A1 35 94 B1 36 EC F8 81 6A C3 A3 {...~...^F...5...6...j..
060: 7B B7 0C 32 A2 C9 42 F3 84 B9 A9 FC 23 6C D9 CA DD CB A8 94 0E 7A B7 37 {...B.....#l.....z.7
078: 4C 54 79 64 B7 2A 99 6E 4C AD 93 CC 4B 86 56 48 B9 BC AE AD D3 E9 D1 62 LTyd.*.nL...K.VH.....b
090: CA 3C BD 86 7D D7 DA A5 FF 86 9C 18 CB 46 63 4C 5A 55 DC E0 50 8A BC 8F <...}.....FcLZU...P...
0A8: 7A 6B 9F A6 99 30 63 B7 07 54 31 30 E8 73 E8 D4 67 C5 E4 AF E2 E6 03 4D zk...0cc..T10.s..g.....M
0C0: C9 87 F7 50 33 51 F6 8D CC 51 E7 B8 3A F9 B8 8E AD 38 3C 2E C6 4F A2 B3 ...P3Q...Q.....8<..0..
0D8: 6A 96 DC 59 C7 61 26 67 3A 67 D0 C7 A9 0E 64 67 4D 9C F6 A6 03 07 95 DA j..Y.a&g:g....dgM.....
0F0: 03 3C 3E 87 CB 12 99 D7 93 B4 30 B4 2B CA 33 3D F3 62 EC C5 8D 24 34 92 <=>.....0.+.=.b...$4.
108: A4 BD BC 62 AF 91 CE 95 86 5F B3 10 FD 9D 5F B2 7D 46 F9 8E 99 3D 81 9A ...b.....)F...=.
120: 4E 57 A6 69 A0 15 50 52 CE 5F CE 53 CB D0 C0 F2 D6 AF 53 DF FC 7B 0E 4F NW.i..PR...S.....S...{.0
138: F0 BD 55 4D 02 80 93 1A F3 4E 58 0A A6 CC 36 FD F5 3F 5D 0D 3D AE 12 C1 ..UM.....NX...6...?}.=...
150: 90 6A 65 4D 47 DB 9A 46 CF 0A 07 9F 26 1E D9 75 6F 8D 92 55 25 DC E2 26 .jeMG..F....&..uo..U%..&
168: 7B 5E 15 FA 63 BD F6 B2 3A 60 DA 67 D6 7C 4A EB F8 53 67 72 D7 AB 56 CE {^..c...:`.g.|J..Sgr..V.
180: B8 57 D4 A8 6F 8E 13 F9 1F FC 1C 5C 20 6F 2C F7 3E 5B 43 C8 3D 36 D1 4B .W..o.....\ o,>[C.=6.K
198: AB 1F 50 DC DF 15 B6 73 D6 B1 5E 0B 89 E7 59 7E 34 31 FA 69 1B 44 85 4A ..P.....s.^...Y~41.i.D.J
1B0: 79 87 BD 1F 7A 12 DE 1A 65 EA 66 4A FF 88 5F 78 C4 F6 3A 86 9D 6E 9D E8 y...z...e.fJ...x...:..n..
1C8: CE 97 5F EB A0 A6 DC CC 03 4C 86 EC B5 98 D7 67 F2 8E F3 80 4C 2A 2D 78 ...L.....L....g....L*-x
1E0: 76 66 F5 5E 42 68 0D 4C 74 0D 71 E1 27 6E C7 39 E6 57 85 0C 53 D0 AE CA vf.^Bh.Lt.q.'n.9.W..S...
1F8: D3 D3 21 76 F9 5F 8E 04 82 8A 90 AE 7B 53 95 8E 0F A1 18 09 42 4E 8B 2B ...!v.....{S.....BN.+
210: 34 A0 52 55 0F EB 45 87 7C 96 F5 BF DB A6 8B 03 97 5C 9E 7F 81 8B 61 ED 4.RU..E.|.....\....a.
228: 26 06 77 52 0B 10 4B E6 A9 6D 4D F8 99 E3 4A C8 BF D2 A2 D0 D7 FD 04 56 &.wR..K..mM...J.....V
240: 47 E3 B7 93 6C B3 60 BE 68 90 F1 25 E7 37 34 68 8E 05 56 A3 5E 2C B9 EC G...l.`.h.%.74h..V.^,..
258: 75 A9 D6 01 D3 83 EF 66 47 3F 17 DE AB EC 3D 24 6C CA 0C FB 77 72 75 B6 u.....fG?....=$l...wru.
270: 0D 8F 58 04 7B 54 68 1F 43 52 75 29 46 51 85 CA ..X.{Th.CRu)FQ..
280:
```

CFB

```
out021.bin out024.bin out025.bin out026.bin out027.bin out028.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000:B0 8D 95 C6 2B 29 94 45 9D 85 43 B6 EB E6 EE 0B 9D 3C B3 8D E1 83 9D 3A .....+).E..C.....<.....:
018:14 0F C7 FF A1 50 FE 64 0D 45 CA C6 B4 A4 16 31 24 DA 27 61 F4 48 DB 75 .....P.d.E.....1$. 'a.H.u
030:41 7B 5B 2F E9 64 1E 6F 42 AA 78 E7 3D C1 3C AA 67 0A B9 68 04 01 8E 1F A{[/.d.oB.x.=.<.g..h....
048:E2 25 4C 4B C4 2B DE 14 64 8D 27 6E 1B E0 E9 B3 12 87 91 D8 A3 62 11 22 .%LK.+..d.'n.....b."
060:C6 32 74 6F AD 13 BE 4A 4B 04 59 99 4B A4 2C E1 5A FE 3C 67 09 09 0C 37 .2to...JK.Y.K.,.Z.<g...7
078:7C AD 27 6E BA 0E FB 8B 0D A3 24 F3 98 08 3C 3A A9 F7 D6 E5 58 98 5F C1 |.'n.....$.<:....X._.
090:E1 F5 83 EE BB 3A DC 7D 9E DD 32 CC A4 AA 69 D5 1D 27 B0 EC E9 6D B4 B4 .....}.2...i...'..m..
0A8:3C B3 F7 14 0E 71 7C 40 44 CF BB 58 E3 F2 27 A7 34 70 23 61 86 32 3F 68 <....q|@D..X...'..4p#a.2?h
0C0:57 C5 42 DD 55 96 D9 90 50 9A 15 02 87 AA 9C A7 6A B9 12 02 36 4B DC BC w.B.U...P.....j...6K..
0D8:B0 C4 24 1A 92 C7 1A 97 A3 DB 98 F9 B7 64 03 E2 3B 83 93 5D E7 8F BA 84 ..$......d.;...].
0F0:EE 05 7D 38 62 66 99 AD D5 34 65 BA 85 3D AB A1 7E C4 E0 0E 8A FE 8A B9 ..}8bf...4e..=..~.....
108:F3 5C 54 80 E4 64 35 E2 72 2F 37 37 7F 1A EC D5 FD DF D4 8C 68 56 A8 20 .\T..d5.r/77.....hV.
120:7A 11 B2 17 1B 88 EF 24 F7 25 8C C1 E0 B9 E4 E9 8B FE D5 0B 92 F5 D7 A8 z.....$.%.....
138:BD 47 4C 42 4A 4C 66 28 BB D2 6D 5A 78 41 EA AD 4F 14 05 FB 4C 10 84 B3 .GLBJLf(..mZxA..0...L...
150:22 9B 40 79 23 F5 6F 16 70 07 1C 1E C0 FC F9 CD D1 28 AF A3 32 7E D3 4A ".@y#.o.p.....(.2~.J
168:71 E6 7B CD 00 BB 61 82 FA A7 93 14 47 F3 18 D9 84 27 40 05 75 D6 ED 70 q.{...a...G...j'@.u..p
180:37 4F C5 C5 66 1B 8D 93 9A BA 5B 84 DA D9 2B 84 59 20 84 77 38 99 F1 DC 70...f.....[...+.Y..w8...
198:73 8B BE 64 85 CB 84 FB 49 98 B0 2B 6F C9 48 37 63 1D E1 11 57 3A 22 70 s..d....I...+o.H7c...W:"p
1B0:41 4A D5 5B B6 8D F6 DB FC 6E 5A F1 43 B8 B3 02 2C 88 98 97 20 5D 76 A7 AJ.[.....nZ.C.....]v.
1C8:AE 5C 22 67 54 6F 35 89 C2 B7 09 03 0B FA 4C F6 DF 29 81 E7 E9 7E 73 0D .\ "gTo5.....L..)...~s.
1E0:73 42 48 55 43 FC 8E 62 42 8B 9F E1 A7 FE 32 FA 01 DA B6 48 F2 20 04 F2 sBHUC..bB.....2....H. ..
1F8:6F F3 39 78 71 15 31 D0 0F 9A E7 17 47 26 D8 7D 65 D6 F2 50 50 3F 78 1E o.9xq.1.....G&..}e..PP?x.
210:80 0E 1B 96 77 94 F0 91 68 F4 36 0E 7D 56 34 2F 98 FE A5 24 1E 13 93 EC ....w...h.6.]V4/...$.
228:F7 A7 C0 34 F7 88 F7 69 EF 53 C0 D3 4C 7B 79 8A B2 39 09 A8 47 72 1B B8 ...4...i.S..L{y..9..Gr..
240:77 57 45 EF D7 8C EA 21 4C 98 98 8C 71 E4 0D 12 1C E8 44 34 A0 C1 2A 4D wWE....!L...q....D4..*M
258:25 DB B3 83 7E 4D C8 EC F6 D0 04 55 FF A7 42 F2 A2 A3 5B 60 98 CD CF 27 %...~M.....U..B...['...'
270:A7 8A 37 45 F6 15 D6 24 E6 B9 99 2F 1B 16 E4 1D ..7E...$.../....
288:
2A0:
```

OFB

```
CancaoDoExilio. out021.bin out024.bin out026.bin out027.bin out028.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000:B0 8D 95 C6 2B 29 94 45 9D 85 43 B6 EB E6 EE 0B 9F B9 AF 1B A8 D3 CA BB .....+).E..C.....
018:7A 64 34 A5 62 16 EF ED 3F CD 3C B5 09 FD F4 DF C8 5B 7F 4B AC 53 13 B4 zd4.b...?.<.....[.K.S..
030:34 A5 F5 F9 6C 05 4F 94 ED 12 11 53 24 51 5C 6A 4B F6 5B F5 AE 0C 1C 69 4...l.O....SSQ\jK.[...i
048:AD F3 A2 D2 87 C2 D9 AB B2 74 2A A9 AB 37 79 FA 3C 47 FC 3F AA 5A A0 22 .....t*...7y.<G.?..Z."
060:81 1D 9C 97 70 81 68 AA F7 C5 36 1A F5 A4 F5 81 DF AC 9E 30 7A 7B D8 FD ....p.h...6.....0z{..
078:18 D9 9C 8A C4 47 B1 F0 66 BC 07 90 2B 1B 3C 03 41 F4 D1 AD 75 4C 0C 0A .....G..f...+.<.A...uL..
090:A9 1D 89 31 5A 0E EE B8 CA 53 BD 37 85 E4 6A 63 95 AA 28 42 98 8D E6 A7 ...1Z....S.7...jc..(B....
0A8:E5 AC 1C D0 C4 93 4C A0 45 64 02 28 33 BD 28 0B 35 BE C1 F4 DE 22 5B DD .....L.Ed.(3.(.5...."[.
0C0:BC 24 05 13 34 57 E4 F8 91 1F 02 C7 9E EF B7 16 0D C2 C5 C4 85 63 A6 FB ..$.4W.....C...
0D8:97 8E 17 ED 1A 95 FA 36 3A 92 78 97 A8 AC 6B 3F 0A 9B 6C E2 75 74 52 5C .....6:..x...k?...l.utR\
0F0:21 DF 0B 73 9C F6 86 63 34 C7 11 F7 6E B7 25 D3 8C 36 65 5F 6E 4A 73 42 !...s...c4...n.%..6e_nJsB
108:3F B9 98 B1 E4 23 D6 3B CD 06 50 47 46 DE 00 4C 92 3B F6 E1 6C 53 E4 B3 ?....#;...PGF...L;...lS..
120:B0 D4 5D 21 F6 B1 CC 2E 09 3A C3 E1 4F 50 33 09 BF 65 11 0C 47 D2 B7 FA ..]!.....OP3...e..G...
138:3E 68 CF BF A9 22 D7 B7 65 01 93 35 EF 11 12 52 CA 18 75 3B 94 3D F1 3D >h...".e..5...R..u;.=.
150:10 30 F6 C9 5E A1 2A 82 0B 66 D3 6A 2E D4 83 F3 CF 95 14 A2 D3 39 68 A6 .0...^.*...f.j.....9h.
168:D2 25 9C 83 17 52 06 C4 B8 F7 83 C9 99 C0 84 93 EA 4E B0 63 39 90 9C 90 .%...R.....N.c9...
180:38 CF E8 17 3F 96 43 45 08 D9 6E B9 2B E5 67 27 B7 F0 D0 F8 EB 72 08 C0 8...?.CE..n.+g'.....r..
198:EC 4E 35 D8 48 7C D2 22 0B 27 A2 E2 50 C9 94 A4 04 D6 CA 95 33 7D B9 4D .N5.H|. ". '...P.....3}.M
1B0:66 BA F6 1E 8C A7 39 61 EF F1 CD 9A B9 6E 57 A0 14 5F 40 77 F6 2E 51 E8 f.....9a.....nW...@w..Q.
1C8:A4 C9 0F FB 6B C2 A9 4A CD 6E E0 A2 F9 55 E4 A5 79 84 1B C3 7E C5 21 50 ....k...J.n...U..y...~.!P
1E0:4A BC 24 09 77 AC 50 50 78 91 C4 C8 4E 1F 6D 94 0E 91 24 61 8A 09 FC BF J.$..w.PPx...N.m...$a....
1F8:E9 A8 6D 18 39 F3 F6 EE 43 02 B9 E7 4E B5 E1 55 11 AC E9 CA 02 8C C7 7F .m.9...C...N..U.....
210:C9 12 4C D6 71 B4 3D 24 15 58 46 1B 92 6A B7 A5 C1 66 92 1B B2 88 45 D0 ..L.q.=$.XF...j...f....E.
228:CB 65 7B FE 8E 08 E0 E6 7C C3 C5 96 4F E3 6F 03 F0 14 96 F9 C2 DA 30 93 .e{.....|...O.o.....0.
240:91 71 26 E0 5F 0F 43 DB E2 45 8F 91 34 2C EE 7F 1D 97 E4 2E F9 D8 DF 74 .q&...C..E..4.....t
258:0D 36 23 19 C3 FE 0D 75 31 16 4F 5A FC 43 9C 08 C5 0C 2D 4A C9 66 72 F4 .#6...u1.OZ.C....-J.fr.
270:44 C0 59 45 9C 4B 1F 3A 05 7E 94 1C 26 1D BB 54 DA 08 20 F3 D.YE.K.:.~...&..T...
288:
```

CTR

AES

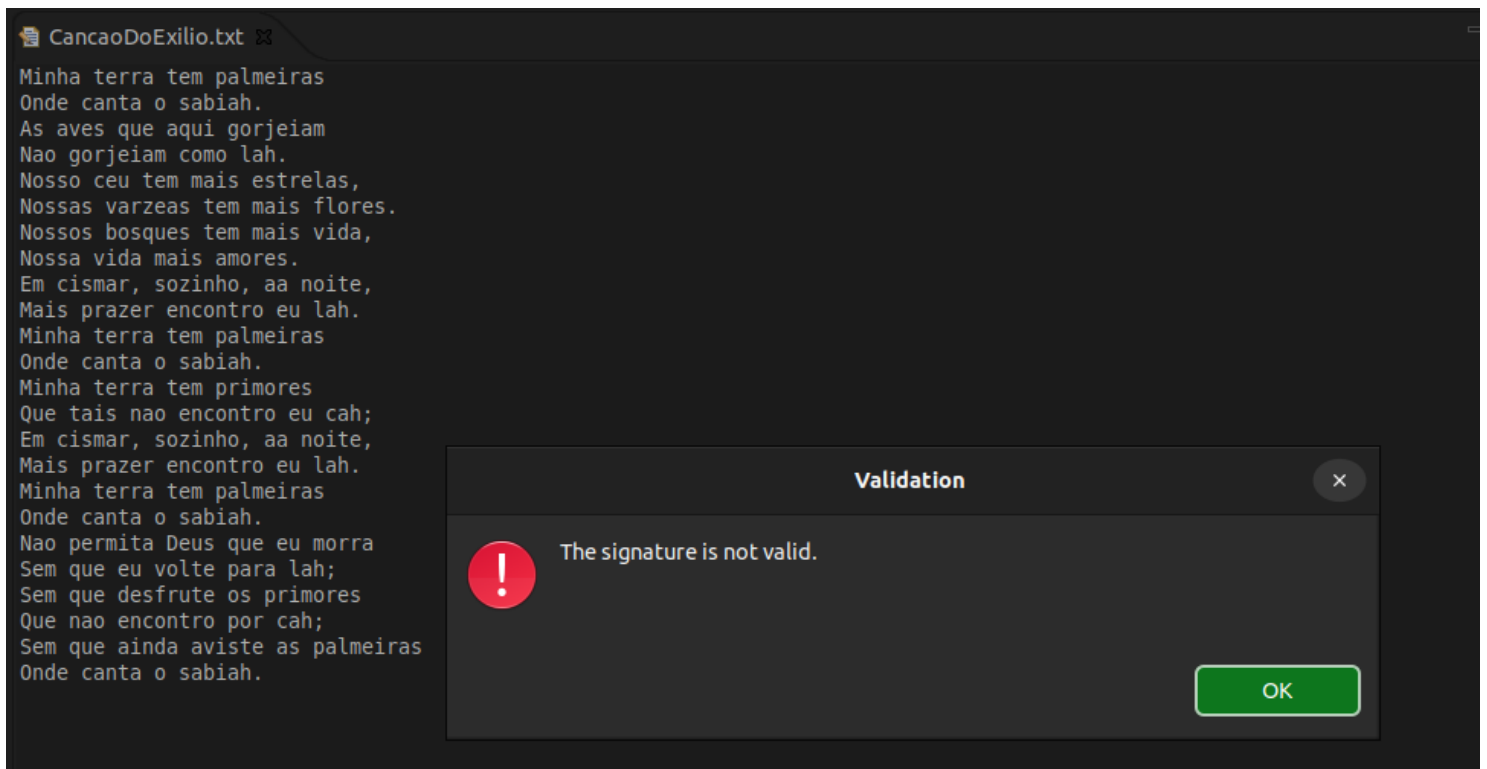
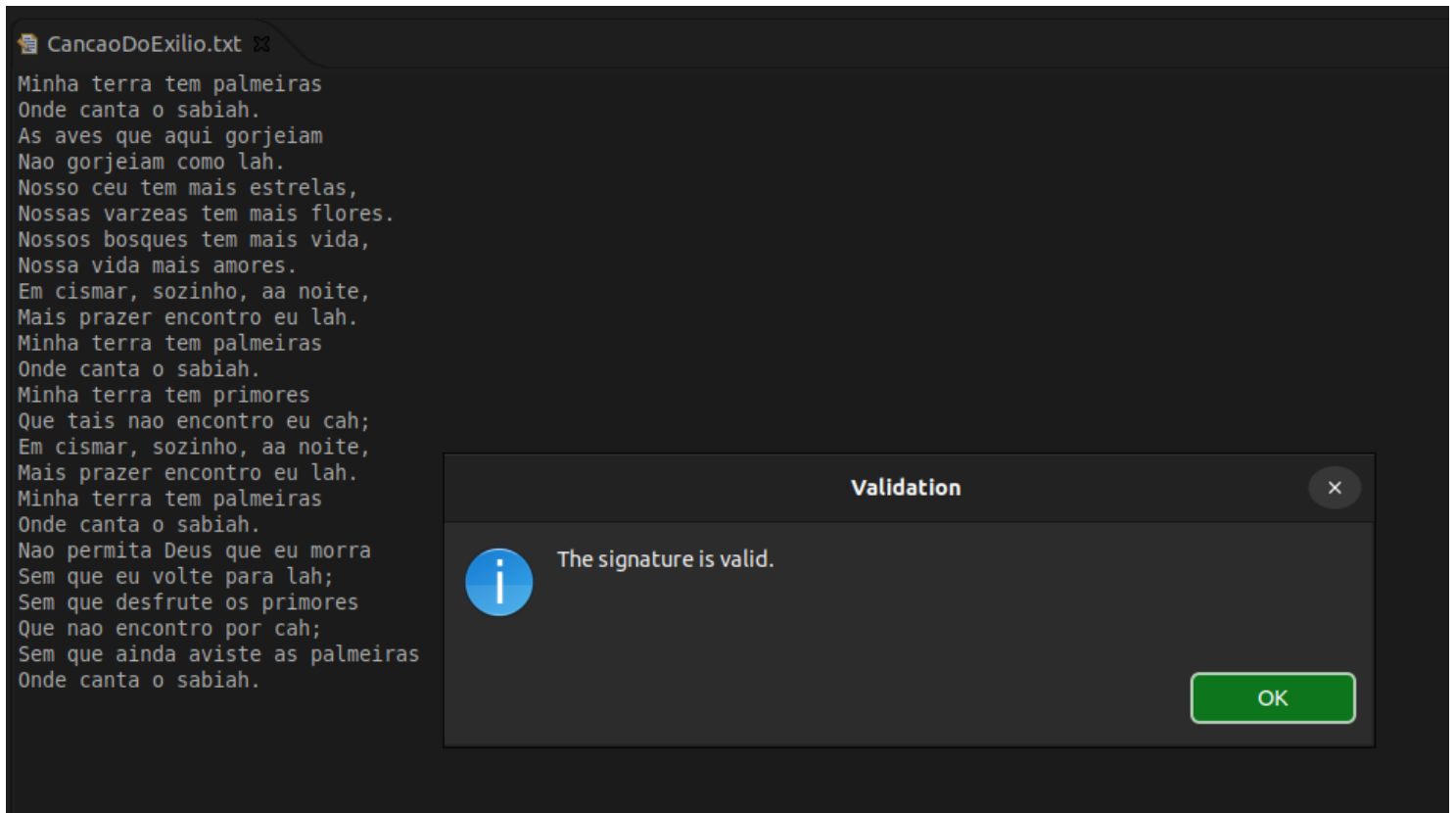
```
20blocostextoclaro.txt  out029.bin  out030.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 .X.)5^h.g=.....X.)5^h.
018: 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB g=.....X.)5^h.g=.....
030: 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 .X.)5^h.g=.....X.)5^h.
048: 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB g=.....X.)5^h.g=.....
060: 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 .X.)5^h.g=.....X.)5^h.
078: 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB g=.....X.)5^h.g=.....
090: 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 .X.)5^h.g=.....X.)5^h.
0A8: 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB g=.....X.)5^h.g=.....
0C0: 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 .X.)5^h.g=.....X.)5^h.
0D8: 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB g=.....X.)5^h.g=.....
0F0: 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 .X.)5^h.g=.....X.)5^h.
108: 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB g=.....X.)5^h.g=.....
120: 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 .X.)5^h.g=.....X.)5^h.
138: 67 3D E0 A2 CF 9A 0C FB 97 58 9D 29 35 5E 68 B1 67 3D E0 A2 CF 9A 0C FB g=.....X.)5^h.g=.....
150:
```

RC6

20blocostextoclaro.txt out029.bin out030.bin

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | |
|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--------------------|--------------------|
| 000: | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 |cB@P..... |
| 018: | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | cB@P.....cB@P..... |
| 030: | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 |cB@P..... |
| 048: | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | cB@P.....cB@P..... |
| 060: | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 |cB@P..... |
| 078: | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | cB@P.....cB@P..... |
| 090: | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 |cB@P..... |
| 0A8: | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | cB@P.....cB@P..... |
| 0C0: | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 |cB@P..... |
| 0D8: | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | cB@P.....cB@P..... |
| 0F0: | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 |cB@P..... |
| 108: | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | cB@P.....cB@P..... |
| 120: | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 |cB@P..... |
| 138: | 63 | 42 | 40 | 50 | DF | 0D | 60 | BC | A9 | 1A | 9C | FD | FA | A4 | 09 | A0 | 63 | 42 | 40 | 50 | DF | 0D | 60 | cB@P.....cB@P..... | |
| 150: | | | | | | | | | | | | | | | | | | | | | | | | | |
| 168: | | | | | | | | | | | | | | | | | | | | | | | | | |

DSA



ECDH

Diffie-Hellman Key Exchange (EC)

The next steps are reachable by the red buttons. Previous settings can be changed by the green buttons.

Watch how Alice and Bob agree on a common secret session key.

Key exchange

Set public parameters

Choose secrets

Create shared keys

Exchange shared keys

Generate common key

Public parameters

$y^2 = x^3 + ax + b$, where
 $a = \text{FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFC}$
 $b = 64210519 \text{ E59C80E7 } 0\text{FA7E9AB } 72243049 \text{ FEB8DEEC } \text{C146B9B}$
field order = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFFFF FFFFFFFF
Generator G = (188DA80E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012 , 7192B95F FC8DA786 31011ED6)

Alice

Secret

a =

Calculate

A = (66af3837fc4e9849b5083e10c88a0c

Calculate

S = 171521f67ed87c81781a724591293e3

Bob

Secret

b =

Calculate

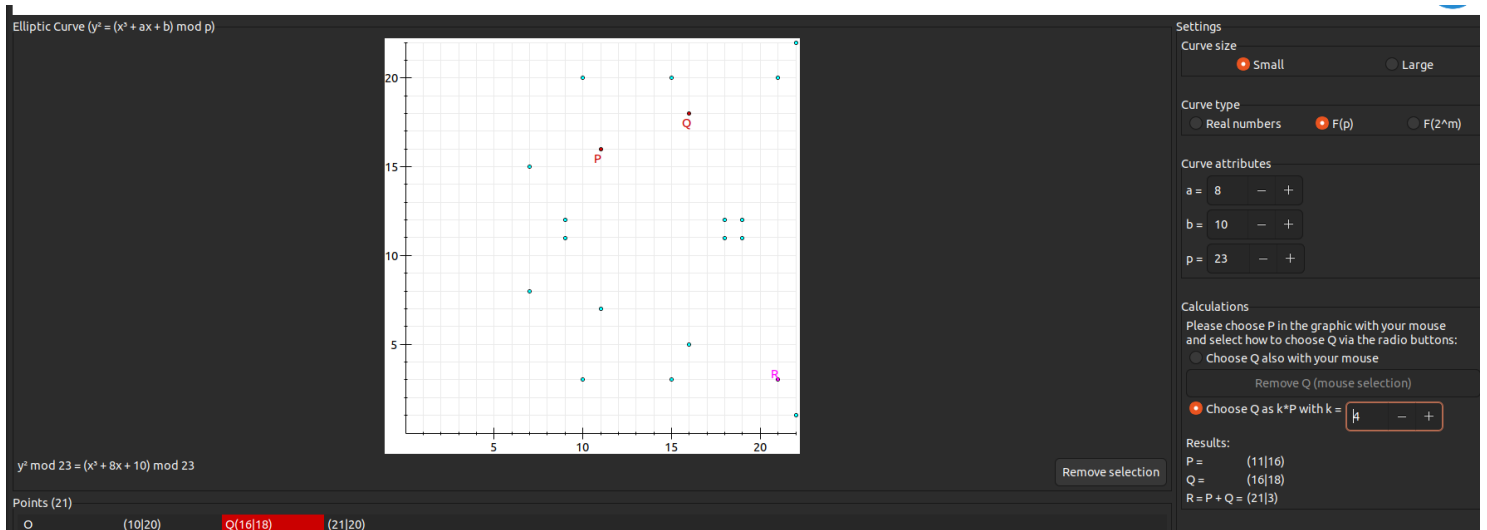
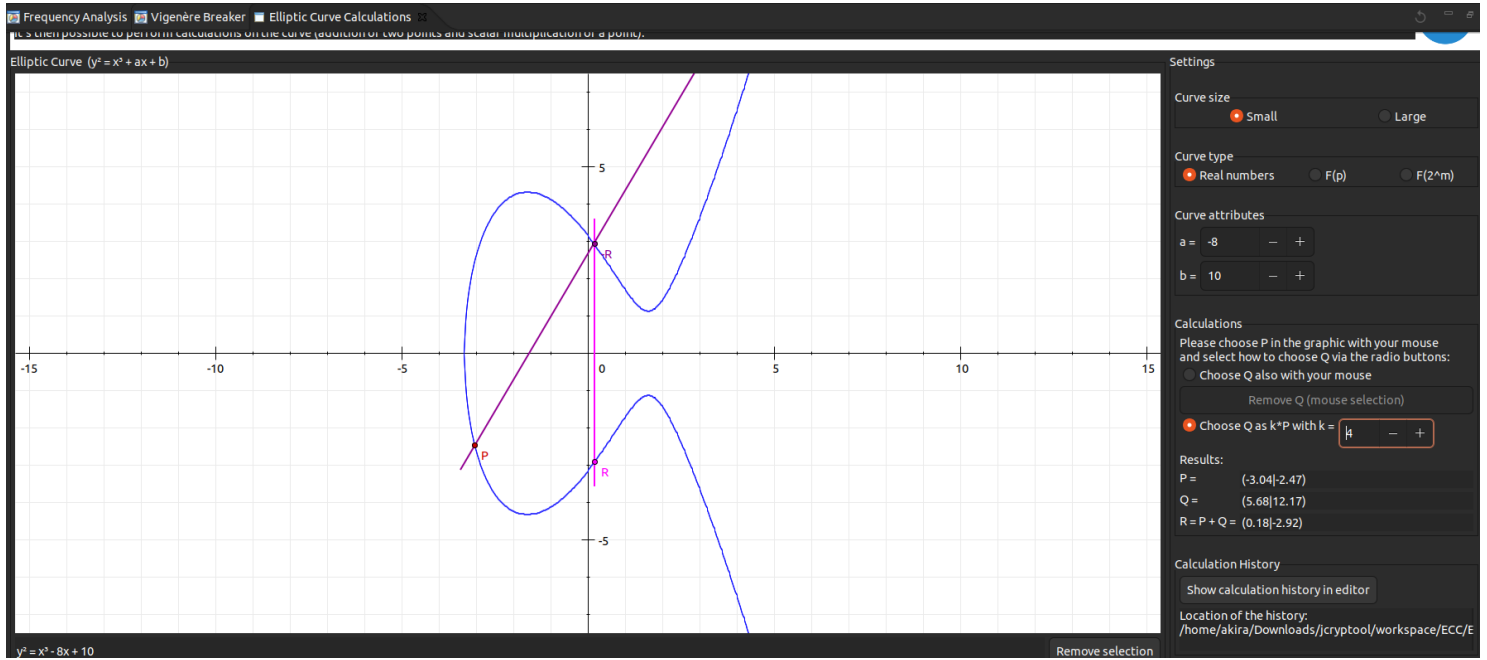
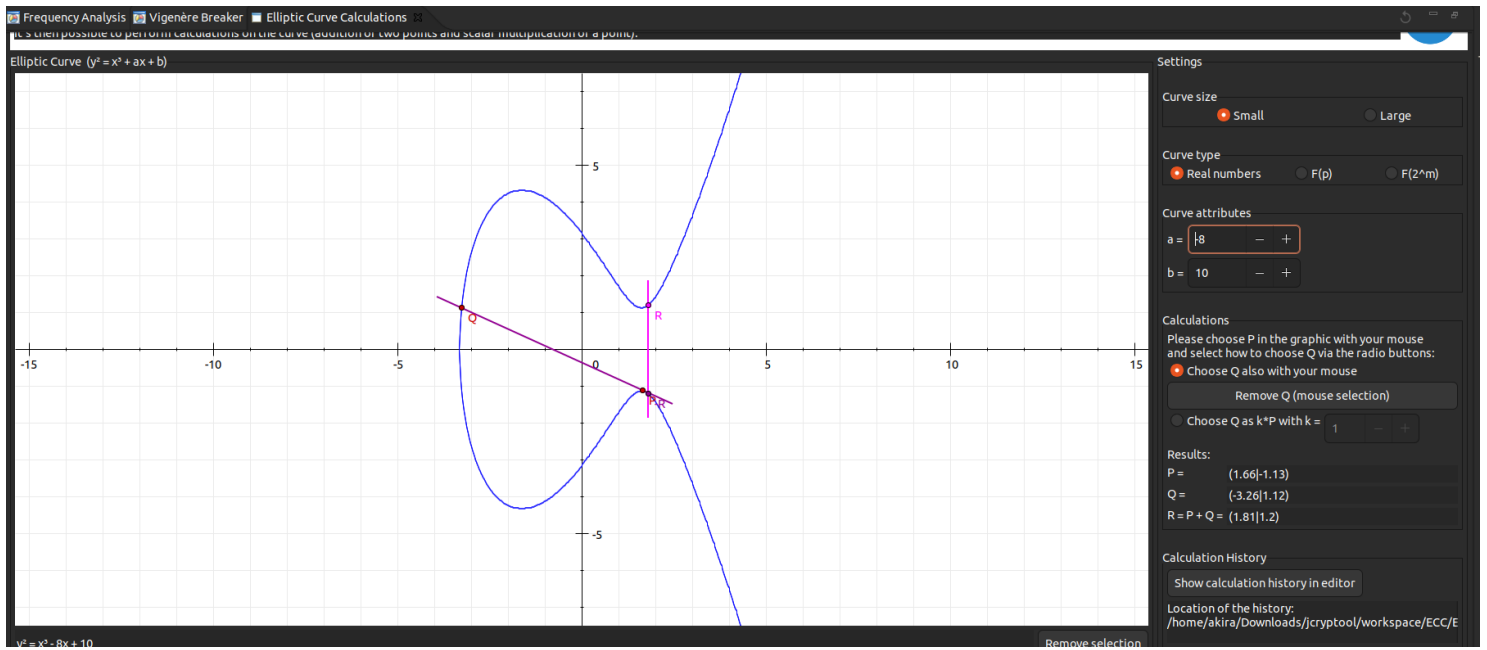
B = (2b914da2ec59535c57205ebb1dadbe

Calculate

S = 171521f67ed87c81781a724591293e3

Save to editor

Save to file



Elliptic Curve Calculations

Elliptic curve

Curve attributes

a = 6277101735386680763835789423207666416083908700390324961276

b = 2455155546008943817740293915197451784769108058161191238065

P = 6277101735386680763835789423207666416083908700390324961279

Basepoint G:

x = 602046282375688656758213480587526111916698976636884684818

y = 174050332293622031404857552280219410364023488927386650641

Order of G = 6277101735386680763835789423176059013767194773182842284081

Point P

Generate random point

Use generator G

x = 525551262866636099314392907814863562264130093076432717249

y = 5750288206841800540373813535574524013312935092400952015711

Point Q

Generate random point

Use generator G

x = 1967015466419347273469142184254343225734331164708701407081

y = 5702394611821311789545398762225240087431815830503689244708

Point R

R = P + 7P = 4P + 4P

x = 2794970062770206927038213404703628894531783728925652998487

y = 1820189860152420674623796758603206258132747217437769894794

Settings

Curve size

Small

Large

Curve type

Real numbers

F(p)

F(2^m)

Select curve attributes

Standard

ANSI X9.62

Curve

prime192v1

Radix

2 (binary)

8 (octal)

10 (decimal)

16 (hexadecimal)

Calculations

Clear points

Add P and Q

Multiply P by k

k = 8

Calculation History

Show calculation history in editor

Location of the history:

/home/akira/Downloads/jcryptool/workspace/ECC/E

Elliptic Curve Calculations

SSL/TLS Handshake

This plug-in serves as graphical representation of a TLS-Handshake. The messages sent are displayed as arrows between client and server. The selectable parameters describe the content of these messages, which are needed to build up the connection.

Client

1. Client Hello

Version

TLS 1.2

Random

639136c126f2cf168a77f46

Generate

Cipher Suite

TLS_RSA_WITH_AES_256_GCM_SHA384

Session ID

0

Information

Next Step

4. Client Certificate

Client Certificate Request

Show

Client Key Exchange

Certificate Verify

Information

Next Step

7. Client Change Cipher Spec

Change Cipher Spec

Parameter

8. Client Finished

Finished

Parameter

Server

2. Server Hello

Version

TLS 1.2

Random

639136ffe8e388f8f78edc2

Generate

Cipher Suite

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Session ID

1

Information

Next Step

3. Server Certificate

Server Certificate

Show

Server Key Exchange

Server Certificate Request

Server Hello Done

Information

Next Step

Server Change Cipher Spec

Change Cipher Spec

Information

Next Step

Server Finished

Finished

Information

Information

Step 8: General explanation of Client Finished

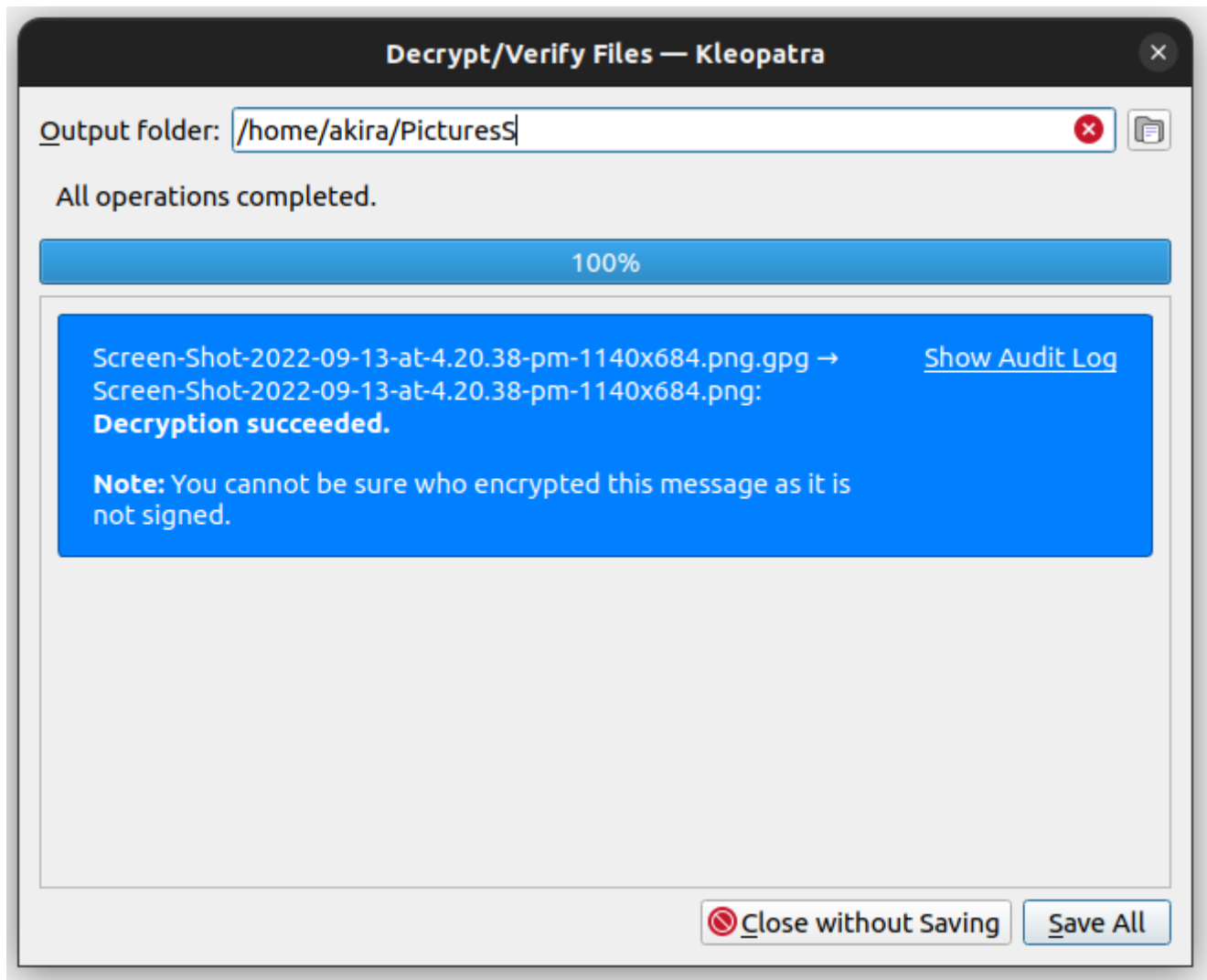
This message is the first encrypted message. It is a hash value from all the previous messages and keys. The Finished-message serves to compare the calculated keys. It is the first message, which is encrypted with the selected parameters. This is displayed with the green arrows.

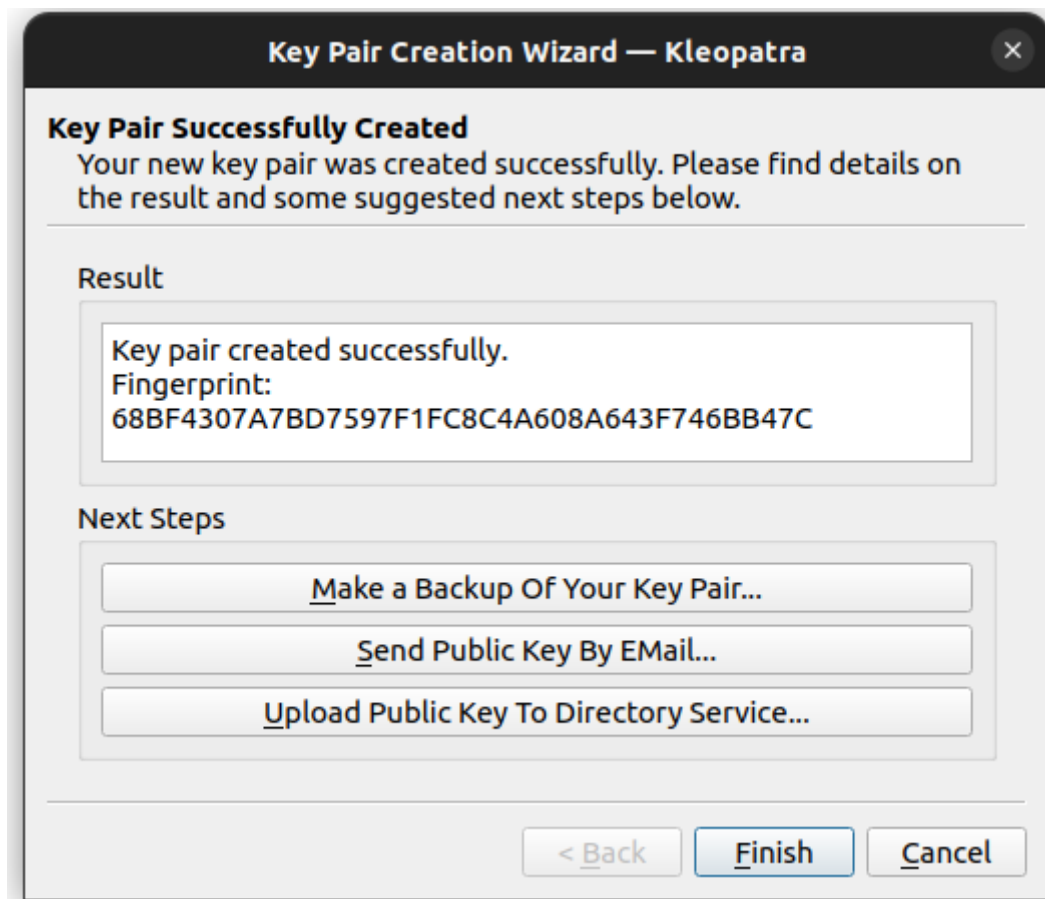
Previous Step

Next Step

Reset

Exercicio 3





Exercicio 4

blake2s256

BLAKE2S-256(stdin)= 6fa16ac015c6513f6b98ee9e3f771ca8324a0ce77fbb9337fe3f8f549643dc73

md4

MD4(stdin)= 8c5b220bf6f482881a90287a64aea150

md5

MD5(stdin)= 68b329da9893e34099c7d8ad5cb9c940

sha1

SHA1(stdin)= adc83b19e793491b1c6ea0fd8b46cd9f32e592fc

ABC - blake2s256

BLAKE2S-256(stdin)= 68296e624aaa1fa5191e3c763911d17700a63258840c5811117f471792b17de8

VICTOR AKIRA - blake2s256

BLAKE2S-256(stdin)= b357cf972b64ac37a56b5599ad15b5599ab28c62da8b607c9398ea15f26a6204

HMAC

HMAC-SHA2-256(CancaoDoExilio.txt)=

ed974ffb0d2e76d9ac5d6aa5df1be27f71d75307ca6e5a40ebabf011d351f399

```
cat CancaoDoExilio.hmac
HMAC-SHA2-256(CancaoDoExilio.txt)=
c61041a6a64d476dcfb78bbde62b50741a5e8d4a89454f298af3ab9c0a7a2cee
```

```
diff CancaoDoExilio.hmac CancaoDoExilio_decrypted.hmac
1c1
< HMAC-SHA2-256(CancaoDoExilio.txt)=
c61041a6a64d476dcfb78bbde62b50741a5e8d4a89454f298af3ab9c0a7a2cee
---
> HMAC-SHA2-256(CancaoDoExilio_decrypted.txt)=
c61041a6a64d476dcfb78bbde62b50741a5e8d4a89454f298af3ab9c0a7a2cee
```

```
-----
cat criptograma.hmac
HMAC-SHA2-256(criptograma.aes)=
b526a5ba74e036295395c15268de341fc093cd0eb5d1cec84dd6b20ea47177e9
```

```
cat criptograma2.hmac
HMAC-SHA2-256(criptograma.aes)=
b526a5ba74e036295395c15268de341fc093cd0eb5d1cec84dd6b20ea47177e9
```

```
openssl enc -d -aes-128-ctr -in criptograma.aes -K 00112233445566778899aabbccddeeff -iv
00998877665544332211feeddccbbaa
```

```
Minha terra tem palmeiras
Onde canta o sabiah.
As aves que aqui gorjeiam
Nao gorjeiam como lah.
Nosso ceu tem mais estrelas,
Nossas varzeas tem mais flores.
Nossos bosques tem mais vida,
Nossa vida mais amores.
Em cismar, sozinho, aa noite,
Mais prazer encontro eu lah.
Minha terra tem palmeiras
Onde canta o sabiah.
Minha terra tem primores
Que tais nao encontro eu cah;
Em cismar, sozinho, aa noite,
Mais prazer encontro eu lah.
Minha terra tem palmeiras
Onde canta o sabiah.
Nao permita Deus que eu morra
Sem que eu volte para lah;
Sem que desfrute os primores
Que nao encontro por cah;
Sem que ainda aviste as palmeiras
Onde canta o sabiah.
```

Os 4 sites retornaram um erro ao tentar se conectar tanto pelo tls 1.2 como pelo tls 1.3

AES - Open SSL

```
openssl enc -e -a -p -aes-256-ctr -pbkdf2 -in textoclaro.txt -out criptograma.aes -k 1234
salt=10AADA2FAAA7999E
key=0AFC38E6712C78FE9BF7ED3239E1D9D59297B298038AA6EA86BA05A49346FCE7
iv =CEF2DF204023929D5AD3F7F03F0FFCD5
```

```
cat criptograma.aes
U2FsdGVkX18QqtovqqeZnn8T6GRENMqnnpaf2yU8A1qpkIq3nTdA2t8eG4T5i9bX
6TNutVzmmagCslPyv+phorMSfrKQw5izvXhI9BUKVKT+1k4PBGJ4gQxx1aWZa+VN
L5hoGhc=
```

```
openssl enc -d -a -p -aes-256-ctr -pbkdf2 -in criptograma.aes -out textoclaro3.txt -k 1234
salt=10AADA2FAAA7999E
key=0AFC38E6712C78FE9BF7ED3239E1D9D59297B298038AA6EA86BA05A49346FCE7
iv =CEF2DF204023929D5AD3F7F03F0FFCD5
```

```
cat textoclaro3.txt
Este eh o texto claro.
Ele carrega informacao sensivel.
Por isto, deve ser protegido.
```

```
openssl enc -e -a -p -aes-256-ctr -in textoclaro.txt -out criptograma.aes -iv
E570548E2B1376147E3342F08082E29A -K
6CB40CAEF6FDEDB31DBD908256F63276DB8FBC1E3430CEF18B6E0F5CD112D5F2
salt=0000000000000000
key=6CB40CAEF6FDEDB31DBD908256F63276DB8FBC1E3430CEF18B6E0F5CD112D5F2
iv =E570548E2B1376147E3342F08082E29A
```

```
cat criptograma.aes
JnBQe28cnflvtIPGg/67SAlivfHMiLY+kFqsygpctg+TYEeLiYnb+mh3rKoPzK9z
PRb1EVa5/46mbGcG5CxYkNzqmXkWlc5C0/ov/duE9n9xbqpMvA==
```

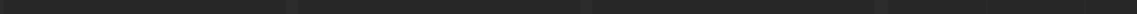
```
openssl enc -d -a -p -aes-256-ctr -in criptograma.aes -out textoclaro2.txt -iv
E570548E2B1376147E3342F08082E29A -K
6CB40CAEF6FDEDB31DBD908256F63276DB8FBC1E3430CEF18B6E0F5CD112D5F2
salt=0000000000000000
key=6CB40CAEF6FDEDB31DBD908256F63276DB8FBC1E3430CEF18B6E0F5CD112D5F2
iv =E570548E2B1376147E3342F08082E29A
```

```
cat textoclaro2.txt
Este eh o texto claro.
Ele carrega informacao sensivel.
Por isto, deve ser protegido.
```

```

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
000: 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 0F AF 8C C4 9F C2 36 13 .....6.&.q.(`.....6.
018: 26 15 71 07 28 60 F9 E2 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 &.q.(`.....6.&.q.(`..
030: 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 0F AF 8C C4 9F C2 36 13 .....6.&.q.(`.....6.
048: 26 15 71 07 28 60 F9 E2 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 &.q.(`.....6.&.q.(`..
060: 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 0F AF 8C C4 9F C2 36 13 .....6.&.q.(`.....6.
078: 26 15 71 07 28 60 F9 E2 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 &.q.(`.....6.&.q.(`..
090: 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 0F AF 8C C4 9F C2 36 13 .....6.&.q.(`.....6.
0A8: 26 15 71 07 28 60 F9 E2 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 &.q.(`.....6.&.q.(`..
0C0: 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 0F AF 8C C4 9F C2 36 13 .....6.&.q.(`.....6.
0D8: 26 15 71 07 28 60 F9 E2 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 &.q.(`.....6.&.q.(`..
0F0: 0F AF 8C C4 9F C2 36 13 26 15 71 07 28 60 F9 E2 00 65 7E A1 40 65 5A 44 .....6.&.q.(`...e~.@eZD
108: 78 27 47 70 5D 42 2F AD                x'Gp]B/.
120:
138:
150:
168:

```

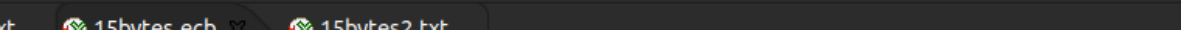
[illegible]

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17

00: 83 48 F0 CC E7 FA CD BC 89 42 95 8F 89 18 FC F3 .H..... .B.....

18:

30:

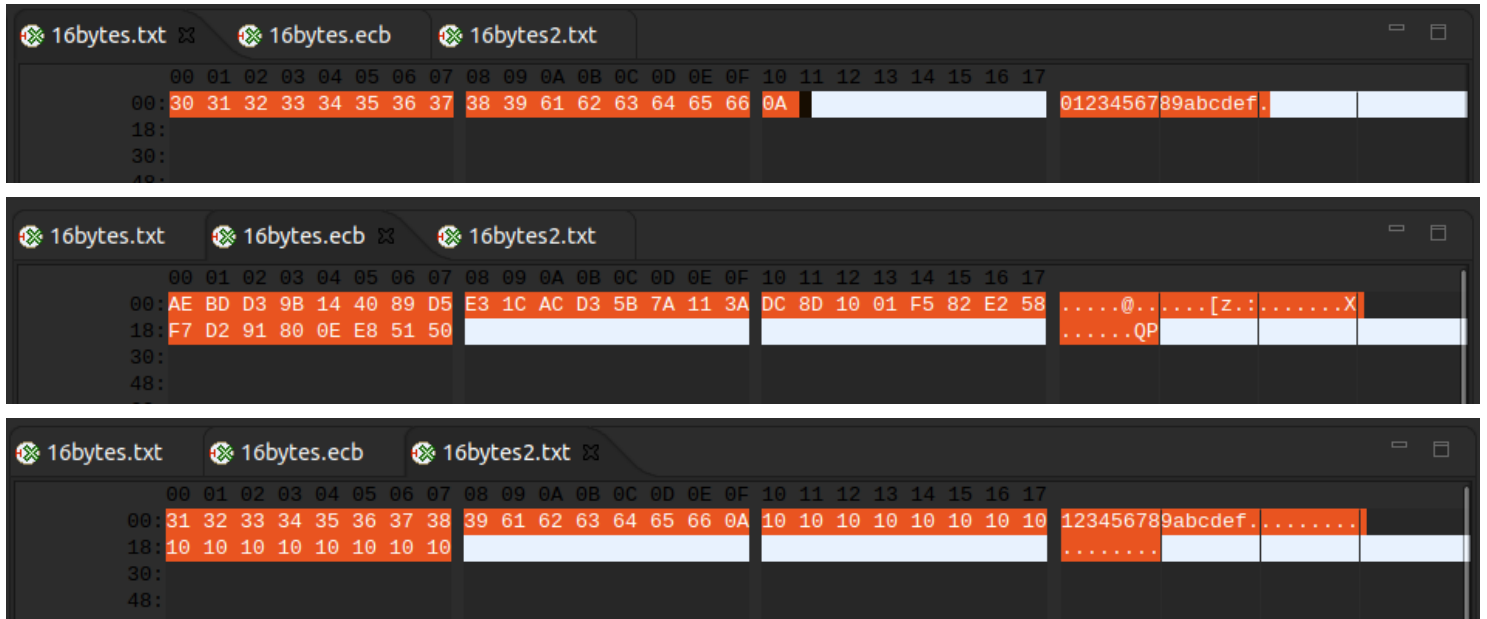
[illegible][illegible]

15bytes.txt 15bytes.ecb 15bytes2.txt

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | |
|-----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----------|--------------------------|
| 00: | 0E | 14 | 8A | 44 | A1 | FD | F4 | 5B | E3 | 74 | 9F | 48 | AB | 74 | B0 | 59 | 00 | 65 | 7E | A1 | 40 | 65 | 5A | 44 | n..D...[.t.H.t.Y.e~.@eZD |
| 18: | 78 | 27 | 47 | 70 | 5D | 42 | 2F | AD | | | | | | | | | | | | | | | | x'Gp]B/. | |
| 30: | | | | | | | | | | | | | | | | | | | | | | | | | |
| 48: | | | | | | | | | | | | | | | | | | | | | | | | | |

15bytes.txt 15bytes.ecb 15bytes2.txt

| Offset | Hex | ASCII |
|--------|-----|-------|
| 00 | 31 | 1 |
| 01 | 32 | 2 |
| 02 | 33 | 3 |
| 03 | 34 | 4 |
| 04 | 35 | 5 |
| 05 | 36 | 6 |
| 06 | 37 | 7 |
| 07 | 38 | 8 |
| 08 | 39 | 9 |
| 09 | 61 | a |
| 0A | 62 | b |
| 0B | 63 | c |
| 0C | 64 | d |
| 0D | 65 | e |
| 0E | 66 | f |
| 0F | 0A | . |
| 10 | 10 | . |
| 11 | 10 | . |
| 12 | 10 | . |
| 13 | 10 | . |
| 14 | 10 | . |
| 15 | 10 | . |
| 16 | 10 | . |
| 17 | 12 | 1 |
| 18 | 34 | 4 |
| 19 | 56 | 8 |
| 1A | 78 | 12 |
| 1B | 9a | a |
| 1C | b | b |
| 1D | c | c |
| 1E | d | d |
| 1F | e | e |



Exercicio 5

O numero 7 do link <https://try-juice-shop.herokuapp.com/rest/basket/7> representa o ID do usuário

Testar com aspas simples ('). O que acontece? Qual o erro?
No results

É possível concatenar partes de uma SQL query e modificar o comando?
Sim

Por que não funciona? O que deu errado?
Query incorreta

Testar o campo da lista de seleção com as opções disponíveis. O que acontece?
Retorna apenas 1 valor

Qual a consulta executada? Qual o resultado da consulta?
Retorna todos os itens da tabela

O que aconteceu com o script injetado?
O script foi executado

Qual campo da mensagem aceita caracteres especiais?
Mensagem

O campo de mensagem aceita tags HTML?
Sim

O campo de mensagem aceita javascript?

Sim

Como o script injetado é ativado?

Ao clicar no título

Como o arquivo é carregado?

Comando cat é executado no servidor

O que aconteceu em cada caso?

A pagina retornou o resultado de cada comando executado

O que acontece se outro comando diferente for digitado?

O Resultado do comando será executado

Testar com: <script>alert(1)<\scrip>. O que aconteceu?

Mensagem de erro

Testar com: 123'); alert(1);(' . O que aconteceu?

Alert executado