

Comunicação Digital

Trabalho Prático

Módulo 1

Nº 49458 Guilherme Barradas

Nº 49219 Gonçalo Carvalho

Nº 48345 José Sequeira

Licenciatura em Engenharia Informática e de Computadores

Semestre de Verão 2022/2023

9/5/2023

Conteúdo

1. Introdução	Erro! Marcador não definido.
2. Resolução do enunciado.....	Erro! Marcador não definido.
Exercício 1	Erro! Marcador não definido.
Exercício 2	Erro! Marcador não definido.
Medições <i>a.txt</i>	Erro! Marcador não definido.
Medições <i>alice29.txt</i>	Erro! Marcador não definido.
Medições <i>cp.html</i>	Erro! Marcador não definido.
Medições <i>lena.bmp</i>	Erro! Marcador não definido.
Medição <i>Person.java</i>	Erro! Marcador não definido.
Medição <i>prog.c</i>	Erro! Marcador não definido.
Medição <i>ListaPalavrasEN.txt</i>	Erro! Marcador não definido.
Medição <i>ListaPalavrasPT.txt</i>	Erro! Marcador não definido.
Exercício 3	Erro! Marcador não definido.
Exercício 4	Erro! Marcador não definido.
Exercício 5	Erro! Marcador não definido.
Conclusão	Erro! Marcador não definido.
Bibliografia	Erro! Marcador não definido.

Índice de Figuras

Figura 1 - Histograma do ficheiro a.txt	8
Figura 2 - Histograma de alice.txt	10
Figura 3 - Histograma de cp.html	13
Figura 4 - Histograma de lena.bmp	16
Figura 5 - Histograma de Person.java	23
Figura 6 - Histograma de prog.c	26
Figura 7 - Histograma de ListaPalavrasEN.txt	29
Figura 8 - Frequência relativa das letras na língua Inglesa	31
Figura 9 - Histograma de ListaPalavrasPT.txt	32
Figura 10 - Frequência Relativa das letras na lingua portuguesa	34
Figura 11 - Histograma do texto plaintext	36
Figura 12 - Histograma do texto encriptado	39
Figura 13 - Sistema com aplicação do modelo de canal binário simétrico	49

1. Introdução

No âmbito da unidade curricular de Comunicação Digital – 2º Ano / 4º Semestre – lecionada pelo docente Vítor Fialho, foi proposta a resolução de diversos exercícios relacionados com a matéria previamente lecionada na cadeira, entre as quais, conceitos como entropia, informação própria, criptografia, entre outros. Nesses exercícios foi desenvolvido código em C e Python que fosse capaz de realizar a tarefa em causa e ainda funções que chamam as mesmas de modo a permitir a realização de testes.

Neste relatório iremos não só apresentar o código realizado como ainda mostrar o seu funcionamento acompanhado de uma explicação breve do processo para obtenção / resolução do mesmo como também, em alguns casos, apresentar resultados obtidos.

2. Resolução do enunciado

Exercício 1

Neste exercício é nos pedida a implementação dos exercícios 4 e 5 da primeira atividade laboratorial realizada anteriormente em contexto de aula. O exercício 4 é realizado em C e é constituído pelas seguintes alíneas:

- (a) Funções `int count_ones(int val)` e `int count_zeros(int val)`, as quais, respetivamente, retornam o número de bits a 1 e a 0 no valor inteiro `val`, passado como parâmetro.
- (b) Função `void print_bits(int val)`, a qual imprime como caracteres os valores dos bits de todos os elementos do valor inteiro `val`, passado como parâmetro.
- (c) Função `char most_frequent_symbol(char *file_name)`, a qual retorna o símbolo mais frequente do ficheiro de texto `file_name`. A função imprime na consola o número de vezes que esse símbolo ocorre no ficheiro.
- (d) Função `void negative_file(char *input_file_name, char *output_file_name)`, a qual transforma o ficheiro de entrada `input_file_name` no ficheiro de saída `output_f`

O código criado de modo a responder a este enunciado pode ser encontrado dentro da pasta em anexo *Lab1* dentro do ficheiro *CFinal.c*. Juntamente com esse mesmo código, acompanhado de cada função vem uma nova função que realiza testes. Alguns dos quais que dão *print* dos resultados e cabe a nós observar se são de facto os valores corretos e outros que automaticamente vão verificar o mesmo e dão *print* relativo a se passou ou não. Neste exercício na função de teste de *negate_file* foi utilizado o ficheiro de teste fornecido *alice29.txt*. Aqui são realizadas duas negações seguidas do ficheiro pelo que se este ficasse desconfigurado era imediatamente notável o erro quando aberto o ficheiro.

No exercício 5 é pedida a realização de código em Python pelo que podem ser observadas as alíneas, constituintes do exercício, abaixo:

- (a) Função que apresenta os primeiros N termos da progressão geométrica de primeiro termo u e razão r. Os valores de N, u e r são passados como parâmetro.
- (b) Função que determina o máximo divisor comum entre dois números inteiros a e b, através do algoritmo de Euclides.
- (c) Função que identifica os símbolos mais frequente e menos frequente de um ficheiro passado como parâmetro, indicando a frequência de ocorrência desses dois símbolos.
- (d) Função que apresenta o histograma de um ficheiro, o valor da informação própria de cada símbolo e a entropia do ficheiro

Aqui, ao contrário dos exercícios realizados em C, não foram realizadas funções de teste, mas foram chamadas as funções realizadas e observados os resultados (que por sua vez podem ser observados em *prints* em funções como *exerD* que realiza a alínea D dando *print* dos valores de histograma numa janela e os valores de informação própria e entropia do ficheiro na consola. A função *exerD* utiliza no seu teste todos os ficheiros de teste fornecidos, à exceção de *ListaPalavrasPT.txt* e *ListaPalavrasEN.txt*.

Exercício 2

Este exercício propõe a resolução de duas alíneas em Python e estas podem ser observadas abaixo:

- (a) Para todos os ficheiros do conjunto TestFilesCD.zip, apresente o histograma, o valor da informação própria de cada símbolo e o valor da entropia do ficheiro.
- (b) Considere os ficheiros ListaPalavrasEN.txt e ListaPalavrasPT.txt, os quais contêm listagens de palavras em Língua Inglesa e Língua Portuguesa. Para cada Língua:
 - (i) Apresente uma estimativa da percentagem de ocorrência de cada símbolo (carater).
 - (ii) Apresente o valor da entropia de ambos os ficheiros.

De modo a realizar a alínea um bastou chamar a função previamente desenvolvida na alínea D do exercício 5 do Laboratório 1, ou seja, *exerD*. Chamando esta para cada um dos ficheiros conseguimos então observar esses mesmos resultados. Vamos então agora observar os mesmos.

Medições *a.txt*

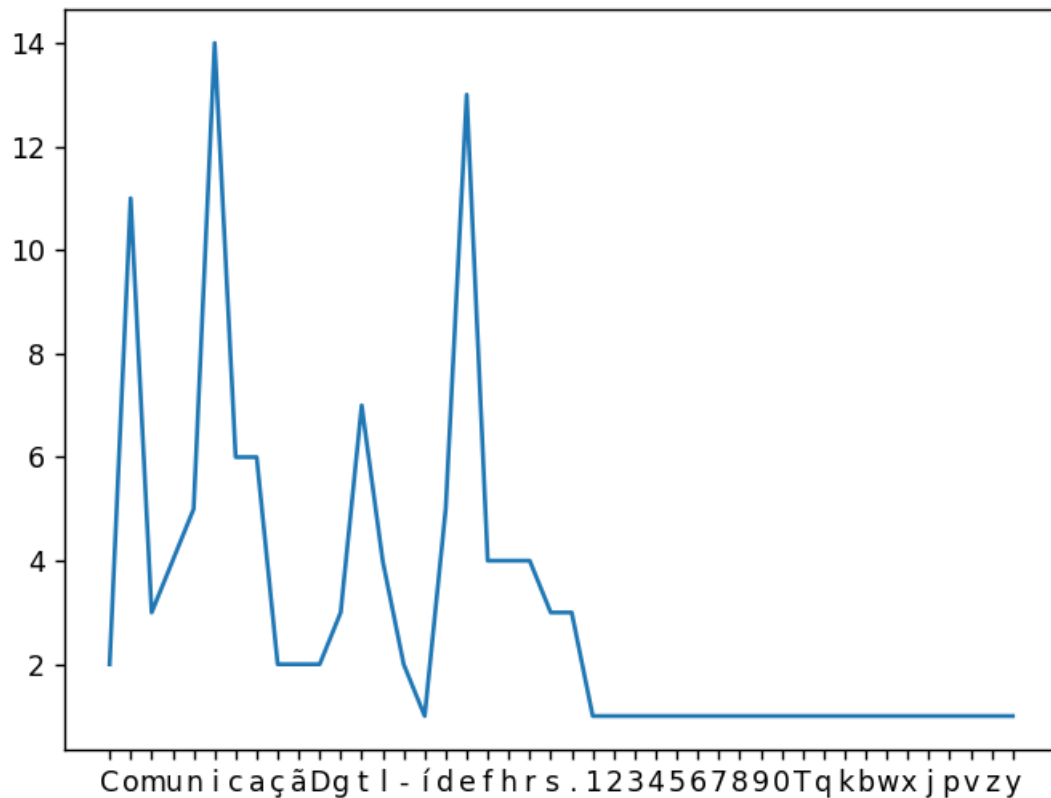


Figura 1 - Histograma do ficheiro *a.txt*

Restantes valores recebidos através de um *print* na consola devidamente identificados.

o valor de informação própria de C: 6.303780748177103

o valor de informação própria de o: 3.844349129539806

o valor de informação própria de m: 5.718818247455947

o valor de informação própria de u: 5.303780748177103

o valor de informação própria de n: 4.9818526532897405

o valor de informação própria de i: 3.496425826119499

o valor de informação própria de c: 4.718818247455947

o valor de informação própria de a: 4.718818247455947

o valor de informação própria de ç: 6.303780748177103

o valor de informação própria de ã: 6.303780748177103

o valor de informação própria de D: 6.303780748177103

o valor de informação própria de g: 5.718818247455947

o valor de informação própria de t: 4.4964258261194985

o valor de informação própria de l: 5.303780748177103

o valor de informação própria de -: 6.303780748177103

o valor de informação própria de í: 7.303780748177103

o valor de informação própria de d: 4.9818526532897405
o valor de informação própria de e: 3.603341030036011
o valor de informação própria de f: 5.303780748177103
o valor de informação própria de h: 5.303780748177103
o valor de informação própria de r: 5.303780748177103
o valor de informação própria de s: 5.718818247455947
o valor de informação própria de .: 5.718818247455947
o valor de informação própria de 1: 7.303780748177103
o valor de informação própria de 2: 7.303780748177103
o valor de informação própria de 3: 7.303780748177103
o valor de informação própria de 4: 7.303780748177103
o valor de informação própria de 5: 7.303780748177103
o valor de informação própria de 6: 7.303780748177103
o valor de informação própria de 7: 7.303780748177103
o valor de informação própria de 8: 7.303780748177103
o valor de informação própria de 9: 7.303780748177103
o valor de informação própria de 0: 7.303780748177103
o valor de informação própria de T: 7.303780748177103
o valor de informação própria de q: 7.303780748177103
o valor de informação própria de k: 7.303780748177103
o valor de informação própria de b: 7.303780748177103
o valor de informação própria de w: 7.303780748177103
o valor de informação própria de x: 7.303780748177103
o valor de informação própria de j: 7.303780748177103
o valor de informação própria de p: 7.303780748177103
o valor de informação própria de v: 7.303780748177103
o valor de informação própria de z: 7.303780748177103
o valor de informação própria de y: 7.303780748177103

O valor de entropia é 4.268499870512438

Medições *alice29.txt*

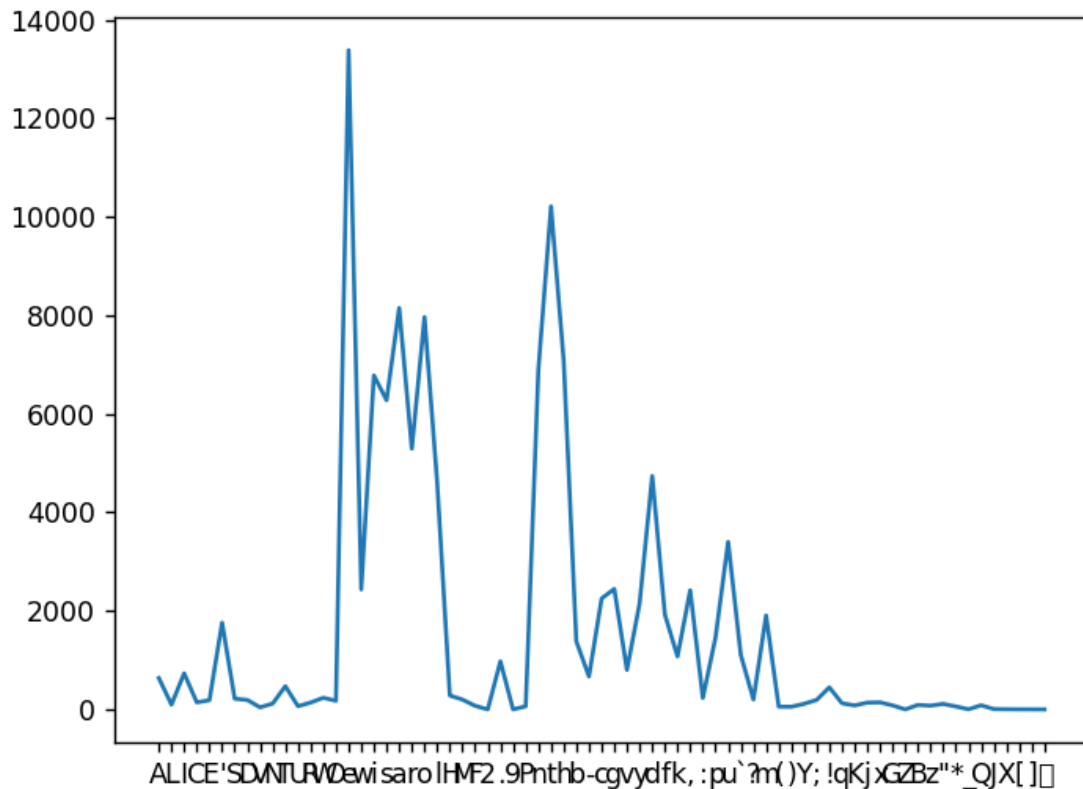


Figura 2 - Histograma de *alice.txt*

Restantes valores recebidos através de um *print* na consola devidamente identificados.

o valor de informação própria de A: 7.8625159089726475

o valor de informação própria de L: 10.565218678622308

o valor de informação própria de I: 7.662259134603706

o valor de informação própria de C: 10.010003521295205

o valor de informação própria de E: 9.62533967105988

o valor de informação própria de ': 6.3977493289063085

o valor de informação própria de S: 9.41174419796059

o valor de informação própria de D: 9.594966022016362

o valor de informação própria de V: 11.787611099958758

o valor de informação própria de N: 10.273037927128998

o valor de informação própria de T: 8.297285473375677

o valor de informação própria de U: 11.135534403379063

o valor de informação própria de R: 10.05064550579255

o valor de informação própria de W: 9.291185273839258

o valor de informação própria de O: 9.72049690410022

o valor de informação própria de e: 3.472030206496347

o valor de informação própria de w: 5.929037987014176

o valor de informação própria de i: 4.4532846012535225
o valor de informação própria de s: 4.564069029154437
o valor de informação própria de a: 4.187521207389019
o valor de informação própria de r: 4.8100585841026415
o valor de informação própria de o: 4.220469876324845
o valor de informação própria de l: 5.007813590204381
o valor de informação própria de H: 9.030181403232834
o valor de informação própria de M: 9.536072332962792
o valor de informação própria de F: 10.970475157108567
o valor de informação própria de 2: 17.179928522737516
o valor de informação própria de .: 7.247713770769132
o valor de informação própria de 9: 17.179928522737516
o valor de informação própria de P: 11.179928522737518
o valor de informação própria de n: 4.429012222759443
o valor de informação própria de t: 3.861950700330399
o valor de informação própria de h: 4.388765634182499
o valor de informação própria de b: 6.746343081587023
o valor de informação própria de -: 7.794066122096057
o valor de informação própria de c: 6.042296924502089
o valor de informação própria de g: 5.9237198342101305
o valor de informação própria de v: 7.530672345220203
o valor de informação própria de y: 6.109807578260694
o valor de informação própria de d: 4.969561577104916
o valor de informação própria de f: 6.268536534894058
o valor de informação própria de k: 7.108466160180893
o valor de informação própria de ,: 5.940329993488394
o valor de informação própria de :: 9.315742378083238
o valor de informação própria de p: 6.67015351841058
o valor de informação própria de u: 5.447761097074133
o valor de informação própria de `: 7.066186356688329
o valor de informação própria de ?: 9.521717039985722
o valor de informação própria de m: 6.282839394424761
o valor de informação própria de (: 11.372573600679914
o valor de informação própria de): 11.398568809212858
o valor de informação própria de Y: 10.347038508572776
o valor de informação própria de ;: 9.580015680550389
o valor de informação própria de !: 8.36935688799637

o valor de informação própria de q: 10.21414423807543
o valor de informação própria de K: 10.822376518119434
o valor de informação própria de j: 10.071404065959348
o valor de informação própria de x: 10.010003521295205
o valor de informação própria de G: 10.822376518119434
o valor de informação própria de Z: 17.179928522737516
o valor de informação própria de B: 10.672133882538821
o valor de informação própria de z: 10.913141982042616
o valor de informação própria de ": 10.35974956032233
o valor de informação própria de *: 11.273037927128998
o valor de informação própria de _ : 15.179928522737518
o valor de informação própria de Q: 10.787611099958758
o valor de informação própria de J: 14.179928522737518
o valor de informação própria de X: 15.179928522737518
o valor de informação própria de [: 16.179928522737516
o valor de informação própria de]: 16.179928522737516
o valor de informação própria de : 17.179928522737516
O valor de entropia é 3.922975614467005

Medições *cp.html*

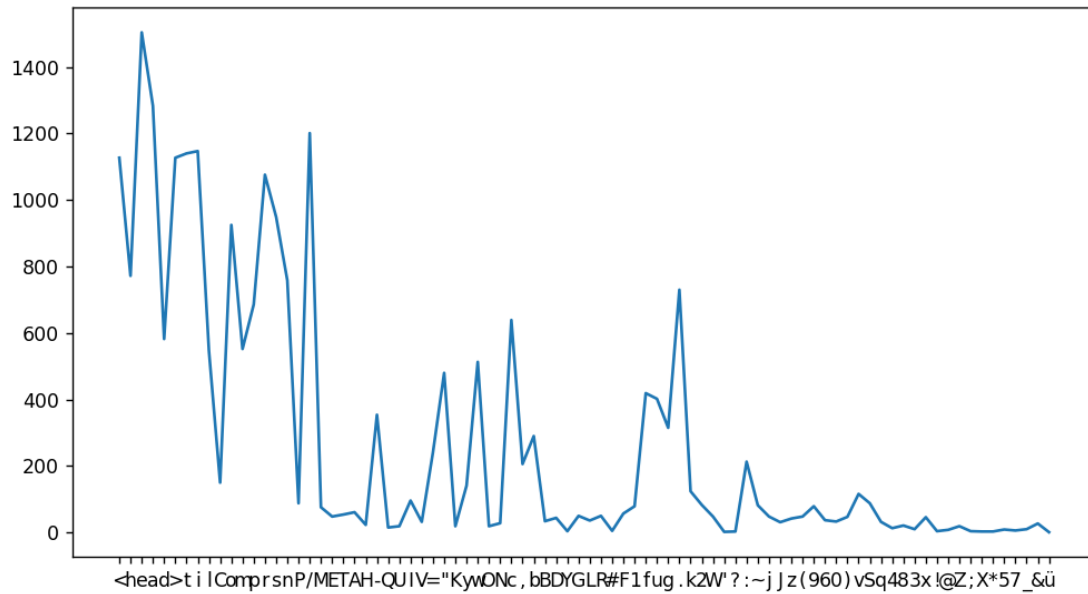


Figura 3 - Histograma de *cp.html*

Restantes valores recebidos através de um *print* na consola devidamente identificados.

o valor de informação própria de <: 4.448274822634284

o valor de informação própria de h: 4.994089585538425

o valor de informação própria de e: 4.031957771128868

o valor de informação própria de a: 4.261241167716823

o valor de informação própria de d: 5.401671279898221

o valor de informação própria de >: 4.448274822634284

o valor de informação própria de t: 4.4317285137544005

o valor de informação própria de i: 4.42289694679068

o valor de informação própria de l: 5.491149600013949

o valor de informação própria de C: 7.357727932310624

o valor de informação própria de o: 4.73323706740283

o valor de informação própria de m: 5.478022166028336

o valor de informação própria de p: 5.164481856633692

o valor de informação própria de r: 4.515084260249881

o valor de informação própria de s: 4.696282345785395

o valor de informação própria de n: 5.020492584635413

o valor de informação própria de P: 8.127115004169207

o valor de informação própria de /: 4.3565261871008705

o valor de informação própria de M: 8.33861910936292

o valor de informação própria de E: 9.00158412208535

o valor de informação própria de T: 8.831659120643037

o valor de informação própria de A: 8.655809285243619
o valor de informação própria de H: 10.062984666749491
o valor de informação própria de -: 6.118941072723508
o valor de informação própria de Q: 10.679656027197986
o valor de informação própria de U: 10.33861910936292
o valor de informação própria de I: 8.00158412208535
o valor de informação própria de V: 9.586546622806505
o valor de informação própria de =: 6.673657286576543
o valor de informação própria de ": 5.679656027197987
o valor de informação própria de K: 10.33861910936292
o valor de informação própria de y: 7.446995270407712
o valor de informação própria de w: 5.583731607199451
o valor de informação própria de O: 10.33861910936292
o valor de informação própria de N: 9.779191700748902
o valor de informação própria de c: 5.266874501859511
o valor de informação própria de ,: 6.900046095623287
o valor de informação própria de b: 6.40663753279157
o valor de informação própria de B: 9.499083781556166
o valor de informação própria de D: 9.127115004169207
o valor de informação própria de Y: 12.586546622806505
o valor de informação própria de G: 8.94269043303178
o valor de informação própria de L: 9.416621621364193
o valor de informação própria de R: 8.94269043303178
o valor de informação própria de #: 12.264618527919142
o valor de informação própria de F: 8.753656608641762
o valor de informação própria de l: 8.282765874629401
o valor de informação própria de f: 5.8757401891071535
o valor de informação própria de u: 5.935494931627576
o valor de informação própria de g: 6.287338604419226
o valor de informação própria de .: 5.074793969039125
o valor de informação própria de k: 7.6323503124196295
o valor de informação própria de 2: 8.21150719145958
o valor de informação própria de W: 9.00158412208535
o valor de informação própria de ': 13.586546622806505
o valor de informação própria de ?: 13.00158412208535
o valor de informação própria de :: 6.851837002580667
o valor de informação própria de ~: 8.228994618188421

o valor de informação própria de j: 9.00158412208535
o valor de informação própria de J: 9.63235031241963
o valor de informação própria de z: 9.194229200027745
o valor de informação própria de (: 9.00158412208535
o valor de informação própria de 9: 8.282765874629401
o valor de informação própria de 6: 9.377093257177554
o valor de informação própria de 0: 9.542152503448051
o valor de informação própria de): 9.031957771128868
o valor de informação própria de v: 7.7285656276789325
o valor de informação própria de S: 8.127115004169207
o valor de informação própria de q: 9.586546622806505
o valor de informação própria de 4: 10.886106904665413
o valor de informação própria de 8: 10.194229200027745
o valor de informação própria de 3: 11.264618527919142
o valor de informação própria de x: 9.062984666749491
o valor de informação própria de !: 12.586546622806505
o valor de informação própria de @: 11.586546622806505
o valor de informação própria de Z: 10.33861910936292
o valor de informação própria de ;: 12.586546622806505
o valor de informação própria de X: 13.00158412208535
o valor de informação própria de *: 13.00158412208535
o valor de informação própria de 5: 11.416621621364193
o valor de informação própria de 7: 12.00158412208535
o valor de informação própria de _: 11.264618527919142
o valor de informação própria de &: 9.831659120643037
o valor de informação própria de ü: 14.586546622806505

O valor de entropia é 4.853373449187902

Medições *lena.bmp*

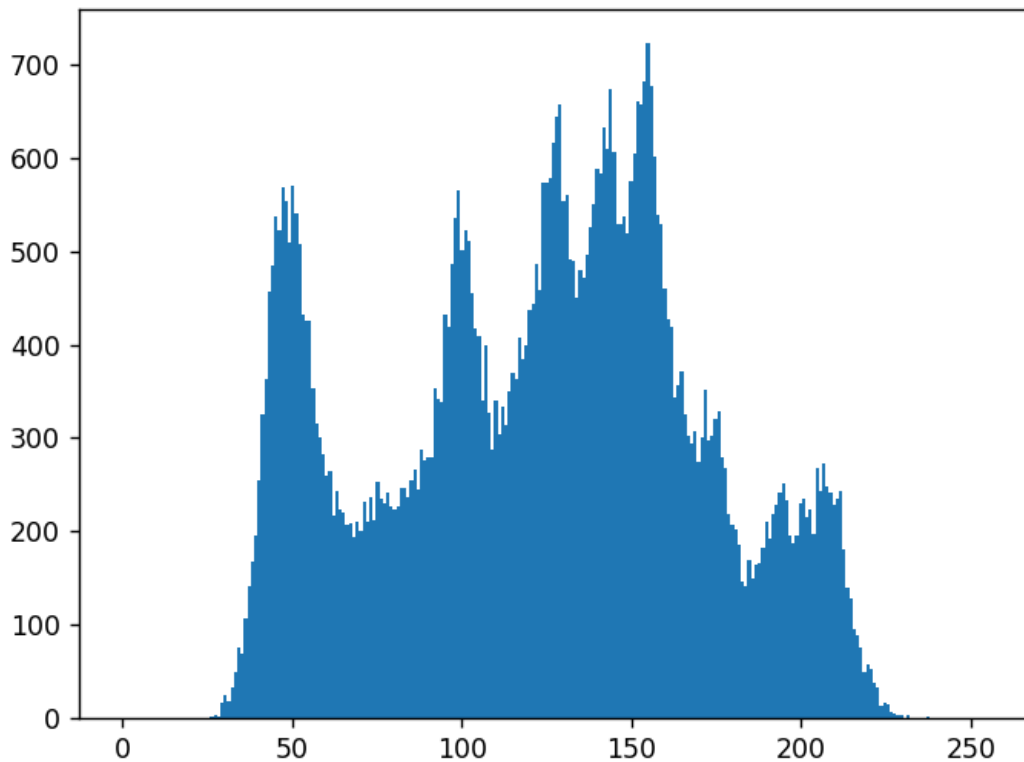


Figura 4 - Histograma de *lena.bmp*

É importante mencionar aqui que uma vez que *lena.bmp* não se trata de um ficheiro de texto, o seu histograma é constituído por valores entre 0 e 255 correspondentes à intensidade da cor preta (a imagem encontra-se a preto e branco) pelo que se obtém o histograma acima.

Restantes valores recebidos através de um *print* na consola devidamente identificados.

o valor de informação própria de 2: 6.693486957499325
o valor de informação própria de 3: 6.108524456778169
o valor de informação própria de 1: 7.693486957499325
o valor de informação própria de 17: 3.6060241162489857
o valor de informação própria de 25: 3.049630767724601
o valor de informação própria de 18: 3.523561956057013
o valor de informação própria de 33: 2.649092838140872
o valor de informação própria de 49: 2.0787771133841173
o valor de informação própria de 75: 1.4646682670034443
o valor de informação própria de 69: 1.584962500721156
o valor de informação própria de 107: 0.9520199710981784
o valor de informação própria de 142: 0.543739837994643
o valor de informação própria de 168: 0.30116953472056474

o valor de informação própria de 196: 0.07877711338411718
o valor de informação própria de 255: -0.3008664793595327
o valor de informação própria de 325: -0.6508089504164916
o valor de informação própria de 363: -0.8103387804964255
o valor de informação própria de 457: -1.1425633975587446
o valor de informação própria de 485: -1.2283539795751648
o valor de informação própria de 538: -1.3779754050572988
o valor de informação própria de 523: -1.3371801787476163
o valor de informação própria de 568: -1.456260162005357
o valor de informação própria de 554: -1.420255208549863
o valor de informação própria de 509: -1.29803488857637
o valor de informação própria de 571: -1.4638599778635175
o valor de informação própria de 540: -1.3833286395515059
o valor de informação própria de 508: -1.2951977292728405
o valor de informação própria de 432: -1.0614005446641432
o valor de informação própria de 426: -1.0412226627265129
o valor de informação própria de 425: -1.0378320735257387
o valor de informação própria de 354: -0.7741185925836722
o valor de informação própria de 315: -0.6057210608879536
o valor de informação própria de 301: -0.5401327192603769
o valor de informação própria de 283: -0.4511712853325571
o valor de informação própria de 259: -0.32332133018722875
o valor de informação própria de 265: -0.3563615919512362
o valor de informação própria de 217: -0.06806427494515412
o valor de informação própria de 244: -0.23725038006356086
o valor de informação própria de 223: -0.1074129424209793
o valor de informação própria de 221: -0.0944156018921065
o valor de informação própria de 207: 0.0
o valor de informação própria de 208: -0.006952760641766901
o valor de informação própria de 194: 0.09357411531219753
o valor de informação própria de 211: -0.027612231207860022
o valor de informação própria de 200: 0.04963076772460074
o valor de informação própria de 232: -0.16449403762824702
o valor de informação própria de 211: -0.027612231207860022
o valor de informação própria de 236: -0.18915609186251603
o valor de informação própria de 212: -0.03443349706387402
o valor de informação própria de 253: -0.289506617194985

o valor de informação própria de 235: -0.18302998906567441
o valor de informação própria de 230: -0.1520030934450501
o valor de informação própria de 242: -0.2253762797752694
o valor de informação própria de 227: -0.13306152979158978
o valor de informação própria de 224: -0.1138679645582788
o valor de informação própria de 226: -0.1266920049158625
o valor de informação própria de 246: -0.2490275478399145
o valor de informação própria de 247: -0.25488027408535235
o valor de informação própria de 237: -0.19525629139893388
o valor de informação própria de 254: -0.29519772927284044
o valor de informação própria de 266: -0.3617954780018643
o valor de informação própria de 245: -0.24315098150324527
o valor de informação própria de 288: -0.4764380439429871
o valor de informação própria de 276: -0.4150374992788438
o valor de informação própria de 279: -0.4306343543298623
o valor de informação própria de 280: -0.43579605944564115
o valor de informação própria de 353: -0.770037415771855
o valor de informação própria de 341: -0.7201409715248472
o valor de informação própria de 338: -0.707392478782859
o valor de informação própria de 432: -1.0614005446641432
o valor de informação própria de 419: -1.0173194762000264
o valor de informação própria de 487: -1.2342910045830169
o valor de informação própria de 536: -1.372602232958447
o valor de informação própria de 566: -1.4511712853325571
o valor de informação própria de 501: -1.2751798356958832
o valor de informação própria de 523: -1.3371801787476163
o valor de informação própria de 511: -1.303692523438296
o valor de informação própria de 455: -1.1362357775867333
o valor de informação própria de 418: -1.0138721745815575
o valor de informação própria de 409: -0.9824700754424234
o valor de informação própria de 340: -0.7159039786383764
o valor de informação própria de 399: -0.9467579787230205
o valor de informação própria de 327: -0.6596598679987571
o valor de informação própria de 287: -0.4714199691763624
o valor de informação própria de 340: -0.7159039786383764
o valor de informação própria de 304: -0.5544405559442604
o valor de informação própria de 333: -0.685891409571937

o valor de informação própria de 314: -0.6011337913923018
o valor de informação própria de 350: -0.7577241543330036
o valor de informação própria de 369: -0.8339900485610707
o valor de informação própria de 363: -0.8103387804964255
o valor de informação própria de 408: -0.9789383844721704
o valor de informação própria de 384: -0.891475543221831
o valor de informação própria de 400: -0.9503692322753993
o valor de informação própria de 437: -1.0780025120012733
o valor de informação própria de 443: -1.0976759310556932
o valor de informação própria de 487: -1.2342910045830169
o valor de informação própria de 459: -1.1488633859144828
o valor de informação própria de 574: -1.4714199691763625
o valor de informação própria de 573: -1.4689043712575796
o valor de informação própria de 579: -1.4839325804899115
o valor de informação própria de 617: -1.5756397216500926
o valor de informação própria de 644: -1.6374299206152918
o valor de informação própria de 657: -1.666262602823004
o valor de informação própria de 554: -1.420255208549863
o valor de informação própria de 561: -1.4383700031094677
o valor de informação própria de 492: -1.2490275478399144
o valor de informação própria de 489: -1.2402036974529083
o valor de informação própria de 450: -1.1202942337177118
o valor de informação própria de 479: -1.2103948882368551
o valor de informação própria de 471: -1.186096292113458
o valor de informação própria de 496: -1.26070935288755
o valor de informação própria de 526: -1.345432031792977
o valor de informação própria de 550: -1.4098008509126965
o valor de informação própria de 588: -1.5061853873370392
o valor de informação própria de 584: -1.4963376013806922
o valor de informação própria de 633: -1.6125747319290158
o valor de informação própria de 609: -1.5568114604070074
o valor de informação própria de 674: -1.7031178236825333
o valor de informação própria de 607: -1.552065748756357
o valor de informação própria de 529: -1.3536369546147005
o valor de informação própria de 529: -1.3536369546147005
o valor de informação própria de 538: -1.3779754050572988
o valor de informação própria de 519: -1.3261037708585557

o valor de informação própria de 575: -1.4739311883324124
o valor de informação própria de 604: -1.5449177818257538
o valor de informação própria de 660: -1.6728352567464904
o valor de informação própria de 657: -1.666262602823004
o valor de informação própria de 682: -1.7201409715248472
o valor de informação própria de 723: -1.8043648794517926
o valor de informação própria de 677: -1.7095250660756713
o valor de informação própria de 601: -1.5377342232118603
o valor de informação própria de 539: -1.3806545052531802
o valor de informação própria de 529: -1.3536369546147005
o valor de informação própria de 460: -1.15200309344505
o valor de informação própria de 427: -1.044605302121165
o valor de informação própria de 419: -1.0173194762000264
o valor de informação própria de 343: -0.7285778086734872
o valor de informação própria de 356: -0.7822464734670728
o valor de informação própria de 372: -0.8456718536087063
o valor de informação própria de 325: -0.6508089504164916
o valor de informação própria de 302: -0.5449177818257538
o valor de informação própria de 294: -0.5061853873370391
o valor de informação própria de 308: -0.5732995831955762
o valor de informação própria de 274: -0.40454512546120164
o valor de informação própria de 300: -0.5353317329965558
o valor de informação própria de 352: -0.7659446611379721
o valor de informação própria de 298: -0.5256815629628362
o valor de informação própria de 303: -0.5496870259736258
o valor de informação própria de 320: -0.6284411373880372
o valor de informação própria de 329: -0.6684568162359162
o valor de informação própria de 279: -0.4306343543298623
o valor de informação própria de 268: -0.3726022329584471
o valor de informação própria de 219: -0.08130010210184817
o valor de informação própria de 207: 0.0
o valor de informação própria de 202: 0.03527547474753053
o valor de informação própria de 186: 0.15432814639129372
o valor de informação própria de 147: 0.49381461266296084
o valor de informação própria de 141: 0.5539356051005316
o valor de informação própria de 170: 0.2840960213616236
o valor de informação própria de 150: 0.46466826700344427

o valor de informação própria de 165: 0.3271647432535095
o valor de informação própria de 166: 0.31844752615240046
o valor de informação própria de 183: 0.17778711921528267
o valor de informação própria de 210: -0.02075856016679749
o valor de informação própria de 192: 0.10852445677816905
o valor de informação própria de 218: -0.07469736727760116
o valor de informação própria de 229: -0.1457168305976187
o valor de informação própria de 241: -0.21940237873063648
o valor de informação própria de 252: -0.2837929660005913
o valor de informação própria de 233: -0.17069918715495488
o valor de informação própria de 196: 0.07877711338411718
o valor de informação própria de 188: 0.1388981058216877
o valor de informação própria de 195: 0.08615664374971455
o valor de informação própria de 230: -0.1520030934450501
o valor de informação própria de 235: -0.18302998906567441
o valor de informação própria de 215: -0.05470589209013505
o valor de informação própria de 223: -0.1074129424209793
o valor de informação própria de 197: 0.07143513804294888
o valor de informação própria de 268: -0.3726022329584471
o valor de informação própria de 244: -0.23725038006356086
o valor de informação própria de 272: -0.3939758837510142
o valor de informação própria de 248: -0.26070935288754993
o valor de informação própria de 242: -0.2253762797752694
o valor de informação própria de 228: -0.13940305666541636
o valor de informação própria de 235: -0.18302998906567441
o valor de informação própria de 243: -0.23132554610645584
o valor de informação própria de 180: 0.20163386116965068
o valor de informação própria de 139: 0.5745458847758179
o valor de informação própria de 128: 0.6934869574993252
o valor de informação própria de 95: 1.1236313491683774
o valor de informação própria de 88: 1.234055338862028
o valor de informação própria de 76: 1.4455594440557396
o valor de informação própria de 50: 2.049630767724601
o valor de informação própria de 57: 1.8605969433345837
o valor de informação própria de 52: 1.993047239358233
o valor de informação própria de 37: 2.4840335918703755
o valor de informação própria de 33: 2.649092838140872

o valor de informação própria de 13: 3.993047239358233
o valor de informação própria de 17: 3.6060241162489857
o valor de informação própria de 14: 3.886132035441721
o valor de informação própria de 7: 4.8861320354417215
o valor de informação própria de 5: 5.371558862611963
o valor de informação própria de 4: 5.693486957499325
o valor de informação própria de 4: 5.693486957499325
o valor de informação própria de 3: 6.108524456778169
o valor de informação própria de 1: 7.693486957499325
A entropia da imagem é 7.424422621459045

Medição *Person.java*

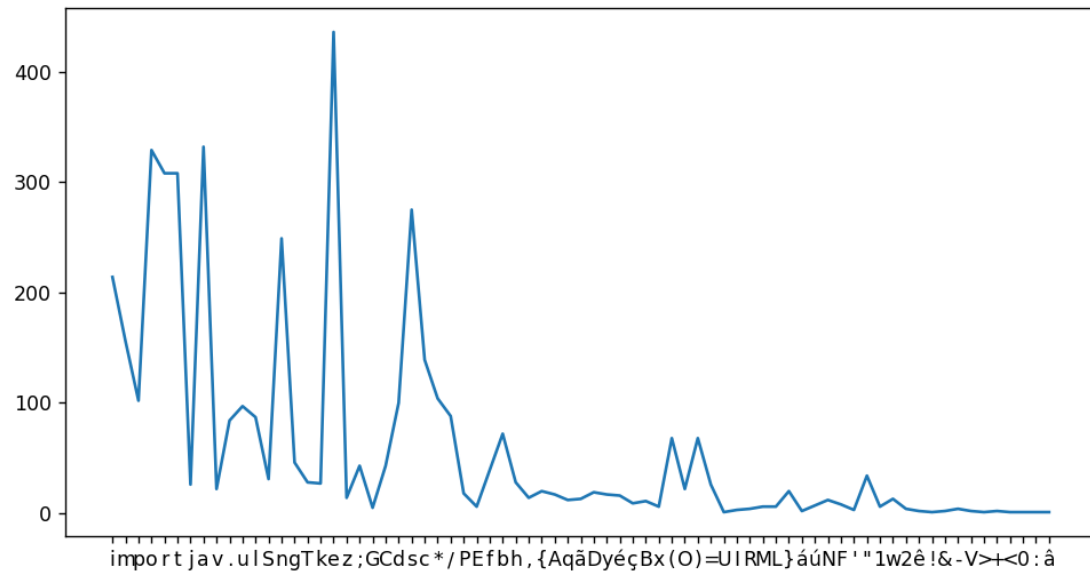


Figura 5 - Histograma de *Person.java*

Restantes valores recebidos através de um *print* na consola devidamente identificados.

- o valor de informação própria de i: 4.888800138625623
- o valor de informação própria de m: 5.3448649061645215
- o valor de informação própria de p: 5.957841783055274
- o valor de informação própria de o: 4.268323351291528
- o valor de informação própria de r: 4.363480584331868
- o valor de informação própria de t: 4.363480584331868
- o valor de informação própria de j: 7.9298274068856776
- o valor de informação própria de a: 4.255227693679845
- o valor de informação própria de v: 8.170835506389473
- o valor de informação própria de .: 6.2379497022480095
- o valor de informação própria de u: 6.0303542828396415
- o valor de informação própria de l: 6.187323629178041
- o valor de informação própria de S: 7.676070814639894
- o valor de informação própria de n: 4.670265192958689
- o valor de informação própria de g: 7.106705168969757
- o valor de informação própria de T: 7.822912202969166
- o valor de informação própria de k: 7.875379622863301
- o valor de informação própria de e: 3.8620828002498433
- o valor de informação própria de z: 8.822912202969166
- o valor de informação própria de ;: 7.204002370324671
- o valor de informação própria de G: 10.308339030139408

o valor de informação própria de C: 7.204002370324671
o valor de informação própria de d: 5.986410935252045
o valor de informação própria de s: 4.526979316614748
o valor de informação própria de c: 5.511326052303263
o valor de informação própria de *: 5.9298274068856776
o valor de informação própria de /: 6.170835506389472
o valor de informação própria de P: 8.460342123584457
o valor de informação própria de E: 10.045304624305613
o valor de informação própria de f: 7.3448649061645215
o valor de informação própria de b: 6.460342123584457
o valor de informação própria de h: 7.822912202969166
o valor de informação própria de ,: 8.822912202969166
o valor de informação própria de {: 8.308339030139408
o valor de informação própria de A: 8.54280428377643
o valor de informação própria de q: 9.045304624305613
o valor de informação própria de ã: 8.929827406885677
o valor de informação própria de D: 8.382339611583184
o valor de informação própria de y: 8.54280428377643
o valor de informação própria de é: 8.63026712502677
o valor de informação própria de ç: 9.460342123584457
o valor de informação própria de B: 9.170835506389473
o valor de informação própria de x: 10.045304624305613
o valor de informação própria de (: 6.54280428377643
o valor de informação própria de O: 8.170835506389473
o valor de informação própria de): 6.54280428377643
o valor de informação própria de =: 7.9298274068856776
o valor de informação própria de U: 12.63026712502677
o valor de informação própria de I: 11.045304624305613
o valor de informação própria de R: 10.63026712502677
o valor de informação própria de M: 10.045304624305613
o valor de informação própria de L: 10.045304624305613
o valor de informação própria de }: 8.308339030139408
o valor de informação própria de á: 11.63026712502677
o valor de informação própria de ú: 9.822912202969166
o valor de informação própria de N: 9.045304624305613
o valor de informação própria de F: 9.63026712502677
o valor de informação própria de ': 11.045304624305613

o valor de informação própria de ": 7.54280428377643
o valor de informação própria de 1: 10.045304624305613
o valor de informação própria de w: 8.929827406885677
o valor de informação própria de 2: 10.63026712502677
o valor de informação própria de ê: 11.63026712502677
o valor de informação própria de !: 12.63026712502677
o valor de informação própria de &: 11.63026712502677
o valor de informação própria de -: 10.63026712502677
o valor de informação própria de V: 11.63026712502677
o valor de informação própria de >: 12.63026712502677
o valor de informação própria de +: 11.63026712502677
o valor de informação própria de <: 12.63026712502677
o valor de informação própria de 0: 12.63026712502677
o valor de informação própria de :: 12.63026712502677
o valor de informação própria de â: 12.63026712502677
O valor de entropia é 3.7244251061297455

Medição *prog.c*

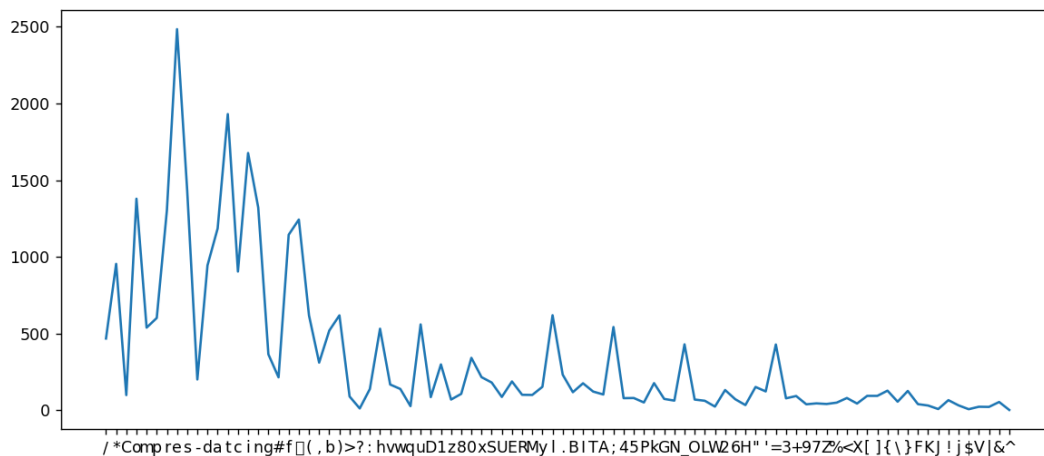


Figura 6 - Histograma de *prog.c*

Restantes valores recebidos através de um *print* na consola devidamente identificados.

o valor de informação própria de /: 6.40637118423403
o valor de informação própria de *: 5.37580446793818
o valor de informação própria de C: 8.658940079828485
o valor de informação própria de o: 4.844243182429712
o valor de informação própria de m: 6.202187561387068
o valor de informação própria de p: 6.042428743232507
o valor de informação própria de r: 4.926028555375558
o valor de informação própria de e: 3.994619787494044
o valor de informação própria de s: 4.789834146679436
o valor de informação própria de -: 7.629793734168968
o valor de informação própria de d: 5.3910068745818505
o valor de informação própria de a: 5.062978580158071
o valor de informação própria de t: 4.358517474993042
o valor de informação própria de c: 5.453470961528504
o valor de informação própria de i: 4.561982950379346
o valor de informação própria de n: 4.9062351726968645
o valor de informação própria de g: 6.765855283744996
o valor de informação própria de #: 7.5321829375425455
o valor de informação própria de f: 5.113778587165303
o valor de informação própria de : 4.994039342891207
o valor de informação própria de (: 6.002186896039317
o valor de informação própria de ,: 6.9975255186694545
o valor de informação própria de b: 6.254059195585811
o valor de informação própria de): 6.002186896039317

o valor de informação própria de >: 8.797916492977294
o valor de informação própria de ?: 11.814218305306396
o valor de informação própria de :: 8.165125467165524
o valor de informação própria de h: 6.221081873139538
o valor de informação própria de v: 7.88994563146964
o valor de informação própria de w: 8.165125467165524
o valor de informação própria de q: 10.5732102058026
o valor de informação própria de u: 6.146945451100502
o valor de informação própria de D: 8.864258987805991
o valor de informação própria de l: 7.05448140348153
o valor de informação própria de z: 9.165125467165524
o valor de informação própria de 8: 8.545729469380493
o valor de informação própria de 0: 6.86002199491952
o valor de informação própria de x: 7.525457074354232
o valor de informação própria de S: 7.781796827614017
o valor de informação própria de U: 8.847385169241594
o valor de informação própria de E: 7.726755464056056
o valor de informação própria de R: 8.629793734168967
o valor de informação própria de M: 8.644293303864083
o valor de informação própria de y: 8.025722410500107
o valor de informação própria de l: 5.999854324729427
o valor de informação própria de .: 7.421900882527635
o valor de informação própria de B: 8.403285204360287
o valor de informação própria de I: 7.822438812111363
o valor de informação própria de T: 8.354786686669097
o valor de informação própria de A: 8.601224581972197
o valor de informação própria de ;: 6.19150088258982
o valor de informação própria de 4: 8.988247705081443
o valor de informação própria de 5: 8.96986917576659
o valor de informação própria de P: 9.629793734168967
o valor de informação própria de k: 7.814218305306395
o valor de informação própria de G: 9.083825365063674
o valor de informação própria de N: 9.319453613556817
o valor de informação própria de _: 6.528816086444147
o valor de informação própria de O: 9.165125467165524
o valor de informação própria de L: 9.342912586380805
o valor de informação própria de W: 10.75008796788668

o valor de informação própria de 2: 8.240226922406242
o valor de informação própria de 6: 9.12390280443901
o valor de informação própria de H: 10.229255804585238
o valor de informação própria de ": 8.035245184618613
o valor de informação própria de ': 8.342912586380805
o valor de informação própria de =: 6.5321829375425455
o valor de informação própria de 3: 9.00686338324879
o valor de informação própria de +: 8.75008796788668
o valor de informação própria de 9: 10.025722410500107
o valor de informação própria de 7: 9.814218305306396
o valor de informação própria de Z: 9.95172182905633
o valor de informação própria de %: 9.658940079828485
o valor de informação própria de <: 8.96986917576659
o valor de informação própria de X: 9.847385169241594
o valor de informação própria de [: 8.734491112835661
o valor de informação própria de]: 8.734491112835661
o valor de informação própria de {: 8.284965237171527
o valor de informação própria de \: 9.492290210419032
o valor de informação própria de }: 8.307865639281605
o valor de informação própria de F: 9.988247705081443
o valor de informação própria de K: 10.366759328335174
o valor de informação própria de J: 12.466295001886088
o valor de informação própria de !: 9.251282110915238
o valor de informação própria de j: 10.319453613556817
o valor de informação própria de \$: 12.688687423222536
o valor de informação própria de V: 10.814218305306396
o valor de informação própria de |: 10.881332501164932
o valor de informação própria de &: 9.545729469380493
o valor de informação própria de ^: 15.273649923943692
O valor de entropia é 4.58129806971062

De modo a realizar a alínea (b) foi criada uma função que pode ser encontrada na pasta *Exer2.b* no ficheiro *main.py*. Esta por sua vez apresenta os resultados de forma semelhante à alínea anterior pelo que obtemos as seguintes medições para cada um dos ficheiros.

Medição *ListaPalavrasEN.txt*

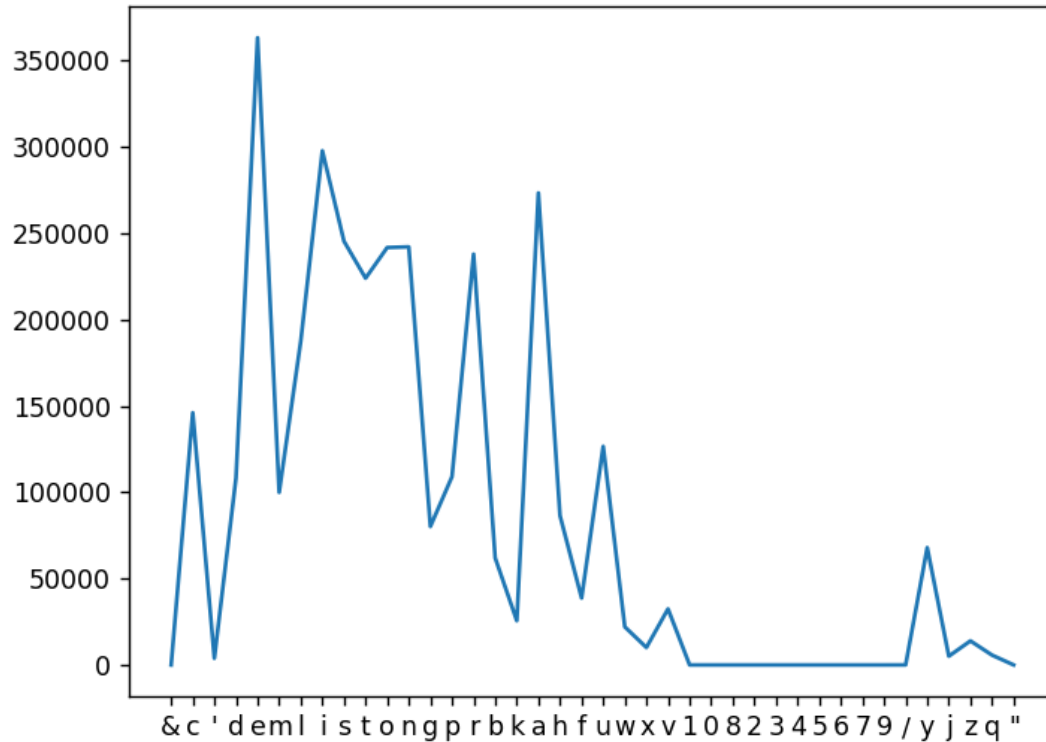


Figura 7 - Histograma de *ListaPalavrasEN.txt*

Embora não tenha sido pedido, uma vez que a implementação seguida para implementação deste exercício partilhava tantas semelhanças com o anterior, adicionámos também a representação gráfica do histograma.

Restantes valores recebidos através de um *print* na consola devidamente identificados.

A percentagem de ocorrência do símbolo: &: 2.9782318059074416e-05%

A percentagem de ocorrência do símbolo: c: 4.350988192204359%

A percentagem de ocorrência do símbolo: ': 0.11540648247891337%

A percentagem de ocorrência do símbolo: d: 3.2219405145848476%

A percentagem de ocorrência do símbolo: e: 10.821047878947981%

A percentagem de ocorrência do símbolo: m: 2.977040513185079%

A percentagem de ocorrência do símbolo: l: 5.587996772788015%

A percentagem de ocorrência do símbolo: i: 8.869561488127129%

A percentagem de ocorrência do símbolo: s: 7.309772144419226%

A percentagem de ocorrência do símbolo: t: 6.671983803184147%

A percentagem de ocorrência do símbolo: o: 7.200560384096599%

A percentagem de ocorrência do símbolo: n: 7.212681787546643%

A percentagem de ocorrência do símbolo: g: 2.388780166882241%
 A percentagem de ocorrência do símbolo: p: 3.2474937434795335%
 A percentagem de ocorrência do símbolo: r: 7.08631541202199%
 A percentagem de ocorrência do símbolo: b: 1.8458187263472554%
 A percentagem de ocorrência do símbolo: k: 0.7629932063554276%
 A percentagem de ocorrência do símbolo: a: 8.142753798213478%
 A percentagem de ocorrência do símbolo: h: 2.5762300767460555%
 A percentagem de ocorrência do símbolo: f: 1.15451155956002%
 A percentagem de ocorrência do símbolo: u: 3.7704414662788213%
 A percentagem de ocorrência do símbolo: w: 0.6569979363831817%
 A percentagem de ocorrência do símbolo: x: 0.3011885825314196%
 A percentagem de ocorrência do símbolo: v: 0.9669723027420283%
 A percentagem de ocorrência do símbolo: l: 0.00011912927223629766%
 A percentagem de ocorrência do símbolo: o: 8.934695417722326e-05%
 A percentagem de ocorrência do símbolo: 8: 5.956463611814883e-05%
 A percentagem de ocorrência do símbolo: 2: 5.956463611814883e-05%
 A percentagem de ocorrência do símbolo: 3: 2.9782318059074416e-05%
 A percentagem de ocorrência do símbolo: 4: 2.9782318059074416e-05%
 A percentagem de ocorrência do símbolo: 5: 2.9782318059074416e-05%
 A percentagem de ocorrência do símbolo: 6: 2.9782318059074416e-05%
 A percentagem de ocorrência do símbolo: 7: 2.9782318059074416e-05%
 A percentagem de ocorrência do símbolo: 9: 2.9782318059074416e-05%
 A percentagem de ocorrência do símbolo: /: 0.0006552109972996372%
 A percentagem de ocorrência do símbolo: y: 2.0235893828418705%
 A percentagem de ocorrência do símbolo: j: 0.15108569951368453%
 A percentagem de ocorrência do símbolo: z: 0.41492725519902485%
 A percentagem de ocorrência do símbolo: q: 0.16964008366448788%
 A percentagem de ocorrência do símbolo: ": 8.934695417722326e-05%

O valor de entropia é 3.9377761467120407

Comparando estes valores obtidos com a frequência relativa das letras na língua inglesa (figura abaixo) podemos então confirmar que os valores apresentam-se muito semelhantes sendo a diferença de apenas algumas casas decimais.













































Letter ♣	Relative frequency in the English language ^[1]			
	Texts ♣		Dictionaries ♣	
A	8.2%		7.8%	
B	1.5%		2%	
C	2.8%		4%	
D	4.3%		3.8%	
E	13%		11%	
F	2.2%		1.4%	
G	2%		3%	
H	6.1%		2.3%	
I	7%		8.6%	
J	0.15%		0.21%	
K	0.77%		0.97%	
L	4%		5.3%	
M	2.4%		2.7%	
N	6.7%		7.2%	
O	7.5%		6.1%	
P	1.9%		2.8%	
Q	0.095%		0.19%	
R	6%		7.3%	
S	6.3%		8.7%	
T	9.1%		6.7%	
U	2.8%		3.3%	
V	0.98%		1%	
W	2.4%		0.91%	
X	0.15%		0.27%	
Y	2%		1.6%	
Z	0.074%		0.44%	

Figura 8 - Frequência relativa das letras na língua Inglesa

Medição *ListaPalavrasPT.txt*

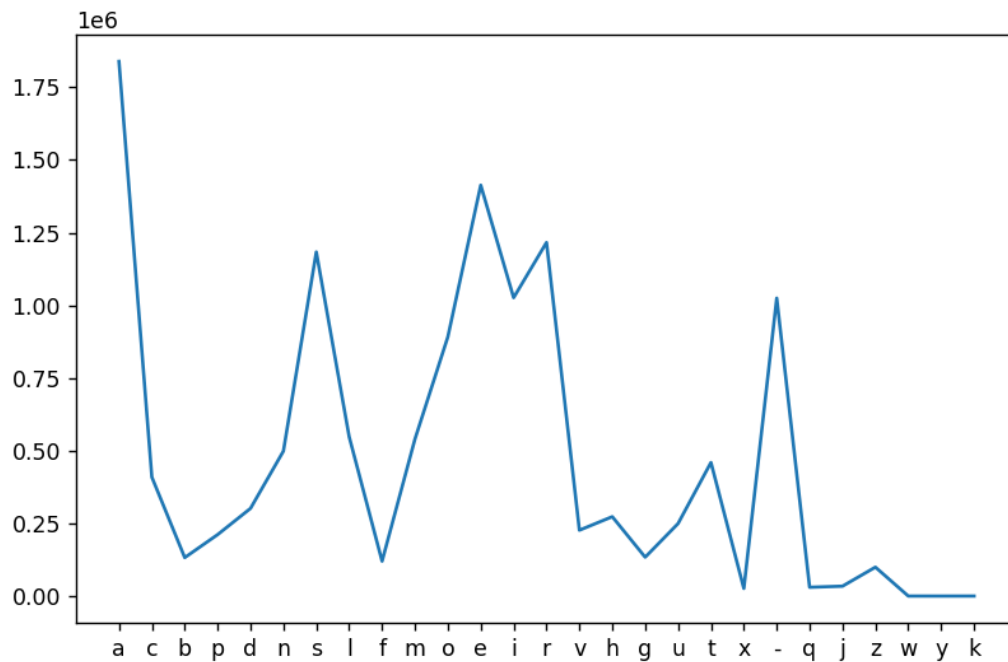


Figura 9 - Histograma de *ListaPalavrasPT.txt*

Restantes valores recebidos através de um *print* na consola devidamente identificados.

A percentagem de ocorrência do símbolo: a: 14.268639834980593%

A percentagem de ocorrência do símbolo: c: 3.173411953899759%

A percentagem de ocorrência do símbolo: b: 1.0269106841765767%

A percentagem de ocorrência do símbolo: p: 1.6407375759322391%

A percentagem de ocorrência do símbolo: d: 2.3402625400436987%

A percentagem de ocorrência do símbolo: n: 3.8688409116562026%

A percentagem de ocorrência do símbolo: s: 9.183145399304376%

A percentagem de ocorrência do símbolo: l: 4.250677140444533%

A percentagem de ocorrência do símbolo: f: 0.9306002317191473%

A percentagem de ocorrência do símbolo: m: 4.190167955654525%

A percentagem de ocorrência do símbolo: o: 6.917603944888545%

A percentagem de ocorrência do símbolo: e: 10.96572271045463%

A percentagem de ocorrência do símbolo: i: 7.961961444012908%

A percentagem de ocorrência do símbolo: r: 9.436965914322872%

A percentagem de ocorrência do símbolo: v: 1.7581874551272032%

A percentagem de ocorrência do símbolo: h: 2.1184265594981775%

A percentagem de ocorrência do símbolo: g: 1.0378178526143653%

A percentagem de ocorrência do símbolo: u: 1.9350914871722469%

A percentagem de ocorrência do símbolo: t: 3.5656278351559143%

A percentagem de ocorrência do símbolo: x: 0.2032875881310458%

A percentagem de ocorrência do símbolo: -: 7.951612821896258%

A percentagem de ocorrência do símbolo: q: 0.2352798801918141%

A percentagem de ocorrência do símbolo: j: 0.26438634959336665%

A percentagem de ocorrência do símbolo: z: 0.7719653189280099%

A percentagem de ocorrência do símbolo: w: 0.0008610922450885743%

A percentagem de ocorrência do símbolo: y: 0.0005430311455513531%

A percentagem de ocorrência do símbolo: k: 0.0012644868103552937%

O valor de entropia é 3.8147694329504858

Mais uma vez podemos comparar com a tabela de frequência relativa e podemos observar a proximidade de valores que mais uma vez confirma o funcionamento correto da função.

Letra ♠	Frequência ♠
a	14.63%
b	1.04%
c	3.88%
d	4.99%
e	12.57%
f	1.02%
g	1.30%
h	1.28%
i	6.18%
j	0.40%
k	0.02%
l	2.78%
m	4.74%
n	5.05%
o	10.73%
p	2.52%
q	1.20%
r	6.53%
s	7.81%
t	4.34%
u	4.63%
v	1.67%
w	0.01%
x	0.21%
y	0.01%
z	0.47%

Figura 10 - Frequência Relativa das letras na língua portuguesa

Exercício 3

No exercício 3 é no pedido que seja realizada uma fonte de símbolos através de C ou Python e acabou por ser escolhido o Python devido a maior facilidade de *debug* e testagem do código. As alíneas podem ser observadas abaixo.

- (a) Implemente uma fonte de símbolos genérica, a qual gera ficheiros com N símbolos, de acordo com a Função Massa de Probabilidade (FMP) do alfabeto de M símbolos: $p(x) = \{p(x_1), p(x_2), \dots, p(x_M)\}$.
- (b) Produza sequências com diferentes dimensões N, para valores de N à sua escolha. Compare o valor da entropia da fonte, $H(X)$, com o valor estimado para a entropia das sequências geradas. Comente os resultados obtidos, em função do par de valores M e N.
- (c) Recorra à implementação da fonte de símbolos, para realizar um gerador de palavras-passe robustas, com dimensão entre 8 e 12 caracteres. Apresente cinco exemplos de palavras-passe

Para cada uma destas foi criado um *script* de Python dentro da pasta *ex3* com o nome correspondente à alínea (*a.py*, *b.py*, *c.py*).

Exercício 4

Neste exercício é pedido para ser feita uma cifra de Vernam para texto. Esta cifra realiza o XOR bit a bit de todos os caracteres de duas sequências: o texto de entrada e uma chave.

- (a) Implemente a função `cypherText = makeVernamCypher(plainText, theKey)`, sendo os parâmetros de entrada e o valor de retorno, sequências de caracteres com a dimensão do texto em claro (`plainText`). Demonstre o (bom) funcionamento fazendo a cifra e a decifra da sequência `abcbcd`, considerando a chave constante e igual a `3333333`.
- (b) Realize a cifra do ficheiro `alice29.txt` (texto em claro) com a chave constante e com chave correspondendo a uma sequência aleatória de caracteres. Para ambas as situações determine os histogramas e entropias do texto em claro e do texto cifrado. Compare os resultados e comente.

Para a alínea a), a função feita cria um array de bytes a partir da key. É calculado quantas vezes a chave, que será convertida em string, tem de se repetir para ter bytes suficientes para cobrir por completo o texto de entrada, para depois ser feito um xor byte a byte dessa chave com o texto lido. Usando a mesma chave no texto de saída podemos decriptar o ficheiro.

Será impresso na consola:

“Texto de entrada:

abcabcd

Texto Encriptado:

RQPRQPW

Texto decriptado:

abcabcd”.

O comportamento para a função em que a cifra gerada é aleatória é semelhante. No entanto, a chave usada pode gerar bytes para o output que não correspondem a caracteres válidos em utf-8. Estes casos são assinalados ao fazer o histograma para o ficheiro de texto encriptado usado esta função, ficando denotados na legenda do eixo horizontal como “iX”, significando a X-ésima ocorrência de um novo “caractere” inválido.

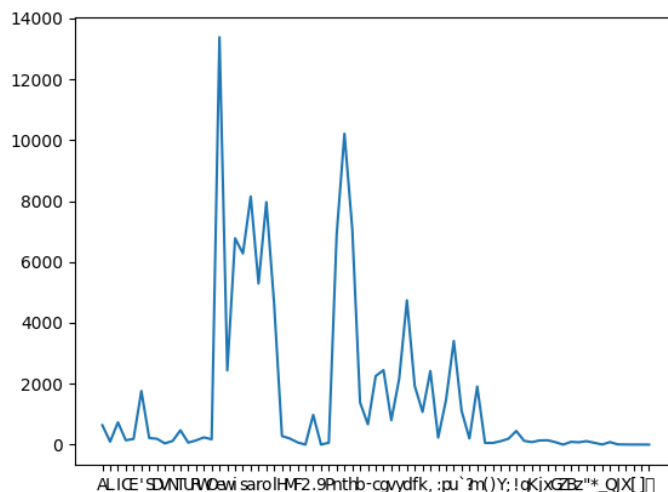


Figura 11 - Histograma do texto plaintext

Restantes valores recebidos através de um *print* na consola devidamente identificados.

o valor de informação própria de A: 7.862506192644076

o valor de informação própria de L: 10.565208962293736

o valor de informação própria de I: 7.662249418275133

o valor de informação própria de C: 10.009993804966632

o valor de informação própria de E: 9.625329954731308

o valor de informação própria de ': 6.397739612577737

o valor de informação própria de S: 9.411734481632019

o valor de informação própria de D: 9.59495630568779

o valor de informação própria de V: 11.787601383630184
o valor de informação própria de N: 10.273028210800426
o valor de informação própria de T: 8.297275757047103
o valor de informação própria de U: 11.135524687050491
o valor de informação própria de R: 10.050635789463978
o valor de informação própria de W: 9.291175557510686
o valor de informação própria de O: 9.720487187771647
o valor de informação própria de e: 3.4720204901677745
o valor de informação própria de w: 5.929028270685604
o valor de informação própria de i: 4.453274884924951
o valor de informação própria de s: 4.564059312825864
o valor de informação própria de a: 4.187511491060447
o valor de informação própria de r: 4.81004886777407
o valor de informação própria de o: 4.220460159996273
o valor de informação própria de l: 5.007803873875808
o valor de informação própria de H: 9.030171686904263
o valor de informação própria de M: 9.53606261663422
o valor de informação própria de F: 10.970465440779995
o valor de informação própria de 2: 17.179918806408946
o valor de informação própria de .: 7.24770405444056
o valor de informação própria de 9: 17.179918806408946
o valor de informação própria de P: 11.179918806408946
o valor de informação própria de n: 4.429002506430871
o valor de informação própria de t: 3.8619409840018264
o valor de informação própria de h: 4.388755917853927
o valor de informação própria de b: 6.746333365258451
o valor de informação própria de -: 7.794056405767484
o valor de informação própria de c: 6.0422872081735175
o valor de informação própria de g: 5.9237101178815585
o valor de informação própria de v: 7.530662628891631
o valor de informação própria de y: 6.1097978619321225
o valor de informação própria de d: 4.9695518607763445
o valor de informação própria de f: 6.268526818565486
o valor de informação própria de k: 7.108456443852321
o valor de informação própria de ,: 5.940320277159822
o valor de informação própria de :: 9.315732661754664
o valor de informação própria de p: 6.670143802082008

o valor de informação própria de u: 5.44775138074556
o valor de informação própria de `: 7.066176640359757
o valor de informação própria de ?: 9.52170732365715
o valor de informação própria de m: 6.2828296780961885
o valor de informação própria de (: 11.37256388435134
o valor de informação própria de): 11.398559092884286
o valor de informação própria de Y: 10.347028792244204
o valor de informação própria de :: 9.580005964221817
o valor de informação própria de !: 8.369347171667798
o valor de informação própria de q: 10.214134521746859
o valor de informação própria de K: 10.822366801790862
o valor de informação própria de j: 10.071394349630776
o valor de informação própria de x: 10.009993804966632
o valor de informação própria de G: 10.822366801790862
o valor de informação própria de Z: 17.179918806408946
o valor de informação própria de B: 10.67212416621025
o valor de informação própria de z: 10.913132265714044
o valor de informação própria de ": 10.359739843993758
o valor de informação própria de *: 11.273028210800426
o valor de informação própria de _: 15.179918806408946
o valor de informação própria de Q: 10.787601383630184
o valor de informação própria de J: 14.179918806408946
o valor de informação própria de X: 15.179918806408946
o valor de informação própria de [: 16.179918806408946
o valor de informação própria de]: 16.179918806408946
o valor de informação própria de SUB: 17.179918806408946
O valor de entropia é 3.9229944461278987

Para o texto cifrado com a chave constante é o seguinte. É de notar que alguns caracteres especiais não renderizados em muitos editores de texto e poderão ser exibidos como um quadrado em branco. No entanto, na consola do PyCharm e VSCode é possível ver que caracteres são esses:

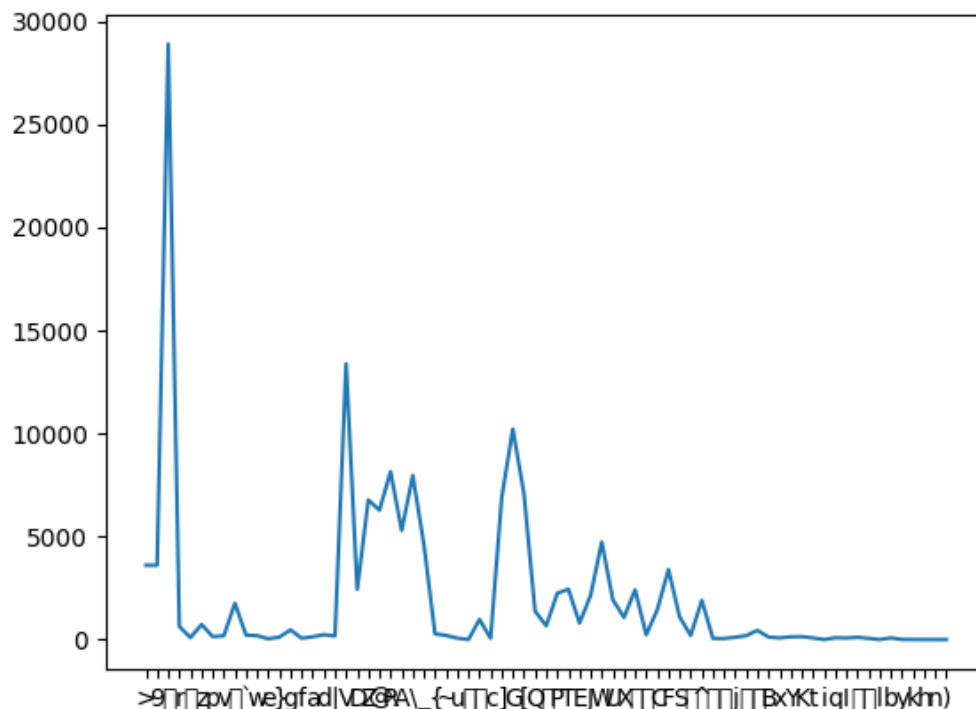


Figura 12 - Histograma do texto encriptado

Restantes valores recebidos através de um *print* na consola devidamente identificados.

o valor de informação própria de >: 5.397572663551332

o valor de informação própria de 9: 5.397572663551332

o valor de informação própria de : 2.3957744145313096

o valor de informação própria de r: 7.897143673041843

o valor de informação própria de • : 10.599846442691504

o valor de informação própria de z: 7.696886898672901

o valor de informação própria de p: 10.044631285364401

o valor de informação própria de v: 9.659967435129076

o valor de informação própria de : 6.432377092975504

o valor de informação própria de `: 9.446371962029787

o valor de informação própria de w: 9.629593786085557

o valor de informação própria de e: 11.822238864027954

o valor de informação própria de } : 10.307665691198196

o valor de informação própria de g: 8.331913237444871

o valor de informação própria de f: 11.17016216744826

o valor de informação própria de a: 10.085273269861746

o valor de informação própria de d: 9.325813037908453

o valor de informação própria de |: 9.755124668169415
o valor de informação própria de V: 3.5066579705655427
o valor de informação própria de D: 5.963665751083372
o valor de informação própria de Z: 4.487912365322719
o valor de informação própria de @: 4.598696793223632
o valor de informação própria de R: 4.222148971458215
o valor de informação própria de A: 4.844686348171837
o valor de informação própria de \: 4.255097640394041
o valor de informação própria de _: 5.042441354273577
o valor de informação própria de {: 9.06480916730203
o valor de informação própria de ~: 9.570700097031988
o valor de informação própria de u: 11.005102921177762
o valor de informação própria de : 17.21455628680671
o valor de informação própria de : 7.282341534838328
o valor de informação própria de c: 11.214556286806713
o valor de informação própria de]: 4.463639986828639
o valor de informação própria de G: 3.8965784643995947
o valor de informação própria de [: 4.423393398251695
o valor de informação própria de Q: 6.780970845656219
o valor de informação própria de -: 7.828693886165253
o valor de informação própria de P: 6.076924688571285
o valor de informação própria de T: 5.958347598279326
o valor de informação própria de E: 7.5653001092893986
o valor de informação própria de J: 6.14443534232989
o valor de informação própria de W: 5.004189341174112
o valor de informação própria de U: 6.303164298963254
o valor de informação própria de X: 7.143093924250089
o valor de informação própria de : 5.97495775755759
o valor de informação própria de : 9.350370142152434
o valor de informação própria de C: 6.704781282479776
o valor de informação própria de F: 5.4823888611433285
o valor de informação própria de S: 7.100814120757525
o valor de informação própria de : 9.556344804054918
o valor de informação própria de ^: 6.317467158493957
o valor de informação própria de : 11.40720136474911
o valor de informação própria de : 11.433196573282054
o valor de informação própria de j: 10.381666272641972

o valor de informação própria de: 9.614643444619585
o valor de informação própria de : 8.403984652065565
o valor de informação própria de B: 10.248772002144626
o valor de informação própria de x: 10.85700428218863
o valor de informação própria de Y: 10.106031830028543
o valor de informação própria de K: 10.044631285364401
o valor de informação própria de t: 10.85700428218863
o valor de informação própria de i: 17.21455628680671
o valor de informação própria de q: 10.706761646608017
o valor de informação própria de I: 10.947769746111812
o valor de informação própria de : 10.394377324391526
o valor de informação própria de : 11.307665691198196
o valor de informação própria de l: 15.214556286806713
o valor de informação própria de b: 10.822238864027954
o valor de informação própria de y: 14.214556286806713
o valor de informação própria de k: 15.214556286806713
o valor de informação própria de h: 16.21455628680671
o valor de informação própria de n: 16.21455628680671
o valor de informação própria de): 17.21455628680671
O valor de entropia é 4.567567024791673

Para o texto cifrado com chave aleatória, os resultados de uma execução são os seguintes:



Pelas dimensões da imagem, esta encontra-se alojada em <https://i.imgur.com/dfuq8do.png> para facilitar a sua leitura.

o valor de informação própria de i0: 8.124443867142425
o valor de informação própria de .: 7.973764954644756
o valor de informação própria de i2: 8.005102921177762
o valor de informação própria de i3: 7.964257868900381
o valor de informação própria de R: 7.976151547481634
o valor de informação própria de 0: 7.992969165541908
o valor de informação própria de w: 7.976151547481634
o valor de informação própria de K: 7.980936610047011
o valor de informação própria de Y: 7.945429607657295
o valor de informação própria de i9: 7.997810428611407

o valor de informação própria de 2: 8.143093924250088
o valor de informação própria de i11: 8.000237166005947
o valor de informação própria de i12: 8.059738177754609
o valor de informação própria de F: 7.966628773363127
o valor de informação própria de i14: 8.137740689755882
o valor de informação própria de 3: 7.952461441436533
o valor de informação própria de i16: 7.964257868900381
o valor de informação própria de i17: 7.997810428611407
o valor de informação própria de i18: 8.121799145886861
o valor de informação própria de i19: 7.992969165541908
o valor de informação própria de i20: 7.976151547481634
o valor de informação própria de q: 8.019799432384465
o valor de informação própria de i22: 8.027204213606216
o valor de informação própria de s: 7.959527716987984
o valor de informação própria de /: 8.00266799226071
o valor de informação própria de a: 8.07500493440792
o valor de informação própria de i26: 7.988144094017928
o valor de informação própria de i27: 8.087851813963523
o valor de informação própria de i28: 8.052164958049808
o valor de informação própria de V: 8.07500493440792
o valor de informação própria de :: 7.943093258902339
o valor de informação própria de i31: 8.000237166005947
o valor de informação própria de ~: 7.985737596310832
o valor de informação própria de c: 7.913060091824164
o valor de informação própria de `: 7.978542094906628
o valor de informação própria de i35: 8.095615214083205
o valor de informação própria de l: 8.039630604306033
o valor de informação própria de i37: 8.027204213606216
o valor de informação própria de 5: 8.012432462976252
o valor de informação própria de i39: 7.940760687592449
o valor de informação própria de O: 7.85700428218863
o valor de informação própria de i41: 8.054684950028324
o valor de informação própria de i42: 8.054684950028324
o valor de informação própria de i43: 8.06480916730203
o valor de informação própria de): 7.983335106095528
o valor de informação própria de i45: 8.119159264014156
o valor de informação própria de i46: 7.913060091824164

o valor de informação própria de i47: 8.034647196791779
o valor de informação própria de i48: 8.022263472335947
o valor de informação própria de i49: 7.978542094906628
o valor de informação própria de i50: 8.039630604306033
o valor de informação própria de i51: 8.037136748817476
o valor de informação própria de i52: 7.957168444114061
o valor de informação própria de i53: 7.906217256667306
o valor de informação própria de g: 8.052164958049808
o valor de informação própria de -: 7.964257868900381
o valor de informação própria de i56: 8.00998514255751
o valor de informação própria de >: 7.964257868900381
o valor de informação própria de <: 8.08269932619792
o valor de informação própria de G: 7.988144094017928
o valor de informação própria de i60: 7.961890854356464
o valor de informação própria de i61: 8.012432462976252
o valor de informação própria de %: 8.062271444500132
o valor de informação própria de A: 8.012432462976252
o valor de informação própria de i64: 8.059738177754609
o valor de informação própria de i65: 8.085273269861746
o valor de informação própria de i66: 7.931467933782711
o valor de informação própria de i67: 7.964257868900381
o valor de informação própria de (: 7.988144094017928
o valor de informação própria de i: 8.00754196662918
o valor de informação própria de i70: 8.100814120757525
o valor de informação própria de i71: 7.943093258902339
o valor de informação própria de i72: 8.093022769466682
o valor de informação própria de i73: 7.964257868900381
o valor de informação própria de i74: 7.961890854356464
o valor de informação própria de }: 8.042128778161231
o valor de informação própria de i76: 7.985737596310832
o valor de informação própria de i77: 7.892628191919351
o valor de informação própria de P: 8.090434974977525
o valor de informação própria de i79: 8.00266799226071
o valor de informação própria de i80: 7.919935537915086
o valor de informação própria de i81: 7.940760687592449
o valor de informação própria de i82: 7.985737596310832
o valor de informação própria de f: 7.917640079927424

o valor de informação própria de i84: 8.029680943898429
o valor de informação própria de i85: 8.022263472335947
o valor de informação própria de i86: 8.000237166005947
o valor de informação própria de i87: 7.961890854356464
o valor de informação própria de i88: 8.00998514255751
o valor de informação própria de i89: 7.971382303333763
o valor de informação própria de i90: 8.032161933402184
o valor de informação própria de y: 8.037136748817476
o valor de informação própria de i92: 8.06480916730203
o valor de informação própria de i93: 8.000237166005947
o valor de informação própria de i94: 8.00754196662918
o valor de informação própria de i95: 8.06480916730203
o valor de informação própria de 6: 8.005102921177762
o valor de informação própria de i97: 8.07500493440792
o valor de informação própria de { : 7.976151547481634
o valor de informação própria de i99: 8.029680943898429
o valor de informação própria de @: 7.988144094017928
o valor de informação própria de X: 7.940760687592449
o valor de informação própria de i102: 8.019799432384465
o valor de informação própria de 7: 7.983335106095528
o valor de informação própria de x: 7.959527716987984
o valor de informação própria de i105: 8.00754196662918
o valor de informação própria de z: 8.05720935144387
o valor de informação própria de B: 7.922234654004674
o valor de informação própria de i108: 7.924537439874094
o valor de informação própria de i109: 7.976151547481634
o valor de informação própria de i110: 7.971382303333763
o valor de informação própria de i111: 8.019799432384465
o valor de informação própria de i112: 8.00754196662918
o valor de informação própria de i113: 8.00754196662918
o valor de informação própria de i114: 7.945429607657295
o valor de informação própria de i115: 8.044631285364401
o valor de informação própria de i116: 7.997810428611407
o valor de informação própria de 4: 7.890375740187972
o valor de informação própria de i118: 8.005102921177762
o valor de informação própria de i119: 7.985737596310832
o valor de informação própria de n: 7.952461441436533

o valor de informação própria de i121: 8.059738177754609
o valor de informação própria de i122: 8.119159264014156
o valor de informação própria de i123: 7.978542094906628
o valor de informação própria de W: 7.980936610047011
o valor de informação própria de i125: 7.957168444114061
o valor de informação própria de i126: 8.042128778161231
o valor de informação própria de i127: 8.017339593696661
o valor de informação própria de i128: 8.037136748817476
o valor de informação própria de i129: 8.080129966585787
o valor de informação própria de i130: 8.032161933402184
o valor de informação própria de i131: 8.00754196662918
o valor de informação própria de i132: 8.052164958049808
o valor de informação própria de i133: 7.926843907257264
o valor de informação própria de i134: 8.093022769466682
o valor de informação própria de i135: 8.027204213606216
o valor de informação própria de i136: 8.121799145886861
o valor de informação própria de v: 7.93378551667611
o valor de informação própria de u: 8.05720935144387
o valor de informação própria de i139: 8.034647196791779
o valor de informação própria de i140: 7.992969165541908
o valor de informação própria de i141: 7.964257868900381
o valor de informação própria de Z: 7.983335106095528
o valor de informação própria de ": 7.964257868900381
o valor de informação própria de p: 8.042128778161231
o valor de informação própria de ?: 7.915348268419434
o valor de informação própria de =: 7.964257868900381
o valor de informação própria de i147: 7.990554612608608
o valor de informação própria de i148: 7.990554612608608
o valor de informação própria de o: 7.924537439874094
o valor de informação própria de i150: 8.06480916730203
o valor de informação própria de \: 8.017339593696661
o valor de informação própria de i152: 7.85700428218863
o valor de informação própria de i153: 7.903943505147185
o valor de informação própria de i154: 8.037136748817476
o valor de informação própria de i155: 8.017339593696661
o valor de informação própria de e: 8.07500493440792
o valor de informação própria de i157: 8.039630604306033

o valor de informação própria de !: 7.969003580551031
o valor de informação própria de i159: 8.000237166005947
o valor de informação própria de i160: 8.042128778161231
o valor de informação própria de i161: 8.014883941970348
o valor de informação própria de i162: 7.985737596310832
o valor de informação própria de J: 8.00754196662918
o valor de informação própria de ^: 7.8994067245504125
o valor de informação própria de i165: 7.8702603788908965
o valor de informação própria de i166: 8.052164958049808
o valor de informação própria de i167: 7.997810428611407
o valor de informação própria de i168: 8.077565174726484
o valor de informação própria de k: 7.952461441436533
o valor de informação própria de i170: 8.116524203846186
o valor de informação própria de h: 8.090434974977525
o valor de informação própria de I: 7.959527716987984
o valor de informação própria de C: 7.938431881532475
o valor de informação própria de i174: 8.077565174726484
o valor de informação própria de : 7.917640079927424
o valor de informação própria de i176: 8.049649360131026
o valor de informação própria de i177: 8.000237166005947
o valor de informação própria de i178: 7.992969165541908
o valor de informação própria de i179: 7.929154067944465
o valor de informação própria de N: 7.990554612608608
o valor de informação própria de Q: 8.07500493440792
o valor de informação própria de L: 8.00266799226071
o valor de informação própria de i183: 7.913060091824164
o valor de informação própria de i184: 8.069898043974831
o valor de informação própria de i185: 8.000237166005947
o valor de informação própria de T: 7.929154067944465
o valor de informação própria de i187: 8.049649360131026
o valor de informação própria de i188: 7.874706283922088
o valor de informação própria de i189: 8.05720935144387
o valor de informação própria de t: 7.917640079927424
o valor de informação própria de D: 7.966628773363127
o valor de informação própria de i192: 8.027204213606216
o valor de informação própria de i193: 7.969003580551031
o valor de informação própria de i194: 7.961890854356464

o valor de informação própria de ,: 7.952461441436533
o valor de informação própria de ': 8.024731727926696
o valor de informação própria de i197: 7.883639408692096
o valor de informação própria de 9: 7.980936610047011
o valor de informação própria de H: 7.959527716987984
o valor de informação própria de i200: 7.91077553862961
o valor de informação própria de i201: 8.047138140974976
o valor de informação própria de i202: 8.012432462976252
o valor de informação própria de i203: 7.931467933782711
o valor de informação própria de i204: 8.06480916730203
o valor de informação própria de i205: 8.014883941970348
o valor de informação própria de i206: 7.8702603788908965
o valor de informação própria de i207: 8.044631285364401
o valor de informação própria de i208: 7.995387766344551
o valor de informação própria de i209: 7.919935537915086
o valor de informação própria de E: 7.91077553862961
o valor de informação própria de d: 8.113893947801515
o valor de informação própria de i212: 7.924537439874094
o valor de informação própria de U: 8.111268478394692
o valor de informação própria de 8: 7.971382303333763
o valor de informação própria de *: 8.090434974977525
o valor de informação própria de \$: 8.05720935144387
o valor de informação própria de i217: 7.924537439874094
o valor de informação própria de &: 8.13240724545284
o valor de informação própria de i219: 8.059738177754609
o valor de informação própria de [: 8.000237166005947
o valor de informação própria de i221: 8.000237166005947
o valor de informação própria de M: 7.997810428611407
o valor de informação própria de i223: 8.037136748817476
o valor de informação própria de i224: 8.111268478394692
o valor de informação própria de i225: 7.908494597378372
o valor de informação própria de S: 7.985737596310832
o valor de informação própria de i227: 7.961890854356464
o valor de informação própria de :: 7.966628773363127
o valor de informação própria de #: 8.005102921177762
o valor de informação própria de i230: 7.983335106095528
o valor de informação própria de i231: 8.119159264014156

o valor de informação própria de r: 8.062271444500132
o valor de informação própria de i233: 8.08269932619792
o valor de informação própria de b: 7.973764954644756
o valor de informação própria de i235: 8.00998514255751
o valor de informação própria de _: 8.08269932619792
o valor de informação própria de +: 7.943093258902339
o valor de informação própria de i238: 8.039630604306033
o valor de informação própria de 1: 8.00754196662918
o valor de informação própria de m: 7.945429607657295
o valor de informação própria de i241: 7.917640079927424
o valor de informação própria de i242: 8.153860355119159
o valor de informação própria de i243: 7.966628773363127
o valor de informação própria de |: 8.014883941970348
o valor de informação própria de i245: 8.085273269861746
o valor de informação própria de i246: 7.841691226694126
o valor de informação própria de i247: 7.952461441436533
o valor de informação própria de i248: 7.885881359478766
o valor de informação própria de i249: 8.143093924250088
o valor de informação própria de i250: 7.91077553862961
o valor de informação própria de i251: 7.995387766344551
o valor de informação própria de j: 7.973764954644756
o valor de informação própria de]: 7.995387766344551
o valor de informação própria de i254: 7.950113686580111
o valor de informação própria de i255: 7.985737596310832
O valor de entropia é 7.9986983434515215

Salta imediatamente à vista o facto de, usando uma chave aleatória em vez de constante, o texto encriptado contem um número muito mais elevado de caracteres, bem como uma entropia maior.

Exercício 5

Por fim, de modo a terminar o exercício foram-nos dadas duas alíneas diretamente ligadas e que podem ser observadas abaixo.

- (a) Escreva uma função tal que implemente o modelo Binary Symmetric Channel (BSC), apresentado na Figura 1. A função recebe: (1) uma sequência binária; (2) o valor pretendido p para o BER. A função deverá retornar a sequência binária resultante da passagem pelo canal. Compare o valor do BER passado como parâmetro (p) com o valor real obtido. Compare os ficheiros recebidos (ponto B) e transmitido (ponto A).
- (b) Considere a técnica de entrelaçamento (interleaving) de transmissão, exemplificada na Figura 2.
- (i) Implemente a técnica de entrelaçamento e comprove o seu funcionamento. Considere que a dimensão da matriz de interleaving é configurável.
- (ii) Tire partido da função BSC implementada na alínea (a) e realize o sistema indicado na Figura 3. Altere as dimensões da matriz de interleaving e relacione com os valores de BER obtidos. Para cada caso compare as sequências nos pontos A e B. Comente os resultados obtidos e compare-os com os da alínea (a).

No primeiro exercício implementamos um sistema que inverte *bits* aleatórios através da probabilidade do BER. É importante, no entanto, mencionar que embora o BER seja um determinado valor, este pode não ser o mesmo que a taxa de erros final. Esta função pode ser encontrada dentro da pasta *Exer5* em *main.py* e ainda *anth.py* com a única diferença entre as implementações ser que o BSC implementado em *main.py* recebe a data através de um ficheiro ao invés de um *string* constituído por zeros e uns.

Para resolver a alínea (b) começámos por realizar a função de *interleaving* que permite que seja dado como *input* a dimensão das linhas e colunas.

Após a implementação de *interleaving* realizámos uma função de *de-interleaving* o que por fim nos permite realizar a alínea (b) ii). Nesta subalínea implementamos, através das funções já desenvolvidas, a figura abaixo.

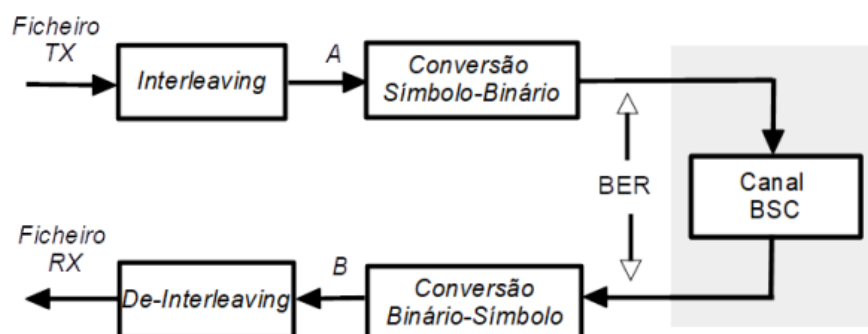


Figura 13 - Sistema com aplicação do modelo de canal binário simétrico

Para implementar este sistema foi criada a função *exer5bii* que permite com maior facilidade testar este sistema para diferentes valores de BER e *strings*. Esta realiza também *print* de diversas fases da data no sistema o que iremos agora realizar para o teste dado com o *string* “ExemploDeTransmissaoInterleaving” para BER de 0.0001 (por exemplo).

Interleaving returns EpensIrvxlTssnlieormatenmDaioeag

Conversão em binário

```
01000101011100000110010101101110011100110100100101110010011101100111100001101
10001010100011100110111001101101110011011000110100101100101011011110111001001
10110101100001011101000110010101101110011011010100010001100001011010010110111
1011001010110000101100111
```

Após BSC

```
01000101011100000110010101101110011100110100100101110010011101100111100001101
10001010100011100110111001101101110011011000110100101100101011011110111001001
10110101100001011101000110010101101110011011010100011001100001011010010110111
1011001010110000101100111
```

Conversão de novo a utf-8 EpensIrvxlTssnlieormatenmFaioeag

De-interleaved é ExemploFeTransmissaoInterleaving

Aqui acima escolhemos demonstrar um caso em que está presente um erro de modo também a demonstrar o correto funcionamento de BSC. Tal como pode ser notado através da leitura do *output* da consola, começamos por realizar o *interleaving* do String, seguidamente, convertemos em binário e passamos pelo BSC. Uma vez isso feito é realizado a conversão de binário para Símbolo e realizamos *de-interleaving* através da função de *interleaving* retornando o resultado final, ou seja, RX.

Comparando o valor inicial e final podemos ver que devido ao baixo BER encontramos apenas um erro nos *bits* após a sua passagem no canal BSC e temos a segurança adicional que é originada pelo processo de interleaving.

Conclusão

Neste trabalho acreditamos que conseguimos com alto nível de sucesso responder a todas as tarefas que nos foram propostas e ainda demonstrar que foram absorvidos todos os conceitos lecionados no decorrer das aulas de Comunicação Digital. Para além disso, acreditamos que os valores obtidos através da testagem de cada um dos programas demonstra que as funções criadas se apresentam, embora por vezes pouco eficientes temporalmente, respondem na totalidade ao que nos é pedido. Um excelente exemplo disso pode ser observado na testagem da frequência de letras nas línguas portuguesas e inglesas onde a diferença entre a data que nos foi fornecida varia apenas em centésimas ou em alguns casos, décimas.

Com tudo isso em conta, acreditamos que este trabalho deixa margem para algumas melhorias no futuro nomeadamente na documentação e testagem do código mas não perdendo o mérito deste primeiro trabalho.

Bibliografia

Wikipedia. (n.d.). Letter frequency. Recuperado em 9 de maio de 2023, de https://en.wikipedia.org/wiki/Letter_frequency?useskin=vector

Wikipedia. (n.d.). Letter frequency. Recuperado em 9 de maio de 2023, de https://en.wikipedia.org/wiki/Letter_frequency?useskin=vector