Relatório de teste de chaves de criptografia.

Link GitHub: https://github.com/Guizith/Sec_FIPS_140-1_TEST

Foi feito um programa em C++ que lê as chaves de criptografia de um arquivo “chaves.txt” e aplica os seguintes testes:

- Teste MonoBit
- Teste Poker
- Teste Runs
- Teste Log Runs

Os respectivos resultados são gravados nos seguintes arquivos:

- Resultados MonoBit.txt
- Resultados PokerTest.txt
- Resultados RunTest.txt
- Resultados LogRunTest.txt

Na figura 1, temos a relação das chaves com cada teste e se a chave é confiável

	MonoBit	Poker	Run	Long Run	Trusted Key
1	R	R	R	A	N
2	R	R	R	A	N
3	R	R	R	A	N
4	R	R	R	A	N
5	R	R	R	A	N
6	R	R	R	A	N
7	R	R	R	A	N
8	R	R	R	A	N
9	R	R	R	A	N
10	R	R	R	A	N
11	A	A	A	A	Y
12	A	A	A	A	Y
13	A	A	A	A	Y
14	A	A	A	A	Y
15	A	A	A	A	Y
16	A	A	A	A	Y
17	A	A	A	A	Y
18	A	A	A	A	Y
19	A	A	A	A	Y
20	A	A	A	A	Y

Figura 1

R = Reprovada

A – Aprovada

N – Não

Y - Sim

Abaixo será discutido os resultados de cada chave em cada teste:

Teste MonoBit

Chave 1 =

Na chave 1 existem 10665 números 1

A chave 1 foi reprovada no teste

Chave 2 =

Na chave 2 existem 10761 números 1

A chave 2 foi reprovada no teste

Chave 3 =

Na chave 3 existem 10677 números 1

A chave 3 foi reprovada no teste

Chave 4 =

Na chave 4 existem 10585 números 1

A chave 4 foi reprovada no teste

Chave 5 =

Na chave 5 existem 10625 números 1

A chave 5 foi reprovada no teste

Chave 6 =

Na chave 6 existem 10578 números 1

A chave 6 foi reprovada no teste

Chave 7 =

Na chave 7 existem 10564 números 1

A chave 7 foi reprovada no teste

Chave 8 =

Na chave 8 existem 10593 números 1

A chave 8 foi reprovada no teste

Chave 9 =

Na chave 9 existem 10788 números 1

A chave 9 foi reprovada no teste

Chave 10 =

Na chave 10 existem 10685 números 1

A chave 10 foi reprovada no teste

Chave 11 =

Na chave 11 existem 10047 números 1

A chave 11 foi aprovada no teste

Chave 12 =

Na chave 12 existem 10065 números 1

A chave 12 foi aprovada no teste

Chave 13 =

Na chave 13 existem 9971 números 1

A chave 13 foi aprovada no teste

Chave 14 =

Na chave 14 existem 10081 números 1

A chave 14 foi aprovada no teste

Chave 15 =

Na chave 15 existem 9926 números 1

A chave 15 foi aprovada no teste

Chave 16 =

Na chave 16 existem 10167 números 1

A chave 16 foi aprovada no teste

Chave 17 =

Na chave 17 existem 10034 números 1

A chave 17 foi aprovada no teste

Chave 18 =

Na chave 18 existem 9944 números 1

A chave 18 foi aprovada no teste

Chave 19 =

Na chave 19 existem 10048 números 1

A chave 19 foi aprovada no teste

Chave 20 =

Na chave 20 existem 9853 números 1

A chave 20 foi aprovada no teste

Teste Poker

-A chave 1 resultou em: 342.828613

Chave Reprovada

-A chave 2 resultou em: 346.924805

Chave Reprovada

-A chave 3 resultou em: 355.449707

Chave Reprovada

-A chave 4 resultou em: 348.607910

Chave Reprovada

-A chave 5 resultou em: 347.744141

Chave Reprovada

-A chave 6 resultou em: 345.919922

Chave Reprovada

-A chave 7 resultou em: 347.936035

Chave Reprovada

-A chave 8 resultou em: 349.715332

Chave Reprovada

-A chave 9 resultou em: 347.967773

Chave Reprovada

-A chave 10 resultou em: 343.238281

Chave Reprovada

-A chave 11 resultou em: 19.539063

Chave Aprovada

-A chave 12 resultou em: 19.123047

Chave Aprovada

-A chave 13 resultou em: 11.487793

Chave Aprovada

-A chave 14 resultou em: 23.993652

Chave Aprovada

-A chave 15 resultou em: 10.969727

Chave Aprovada

-A chave 16 resultou em: 17.011230

Chave Aprovada

-A chave 17 resultou em: 11.846191

Chave Aprovada

-A chave 18 resultou em: 13.139160

Chave Aprovada

-A chave 19 resultou em: 33.811035

Chave Aprovada

-A chave 20 resultou em: 24.428711

Chave Aprovada

Teste Run

- Chave 1

Número de sequencias de tamanho 1:

0 = 2757

1 = 2555

Número de sequencias de tamanho 2:

0 = 1403

1 = 1325

Número de sequencias de tamanho 3:

0 = 702

1 = 690

Número de sequencias de tamanho 4:

0 = 268

1 = 334

Número de sequencias de tamanho 5:

0 = 85

1 = 163

Número de sequencias de tamanho 6+:

0 = 29

1 = 177

Chave Reprovada

- Chave 2

Número de sequencias de tamanho 1:

0 = 2757

1 = 2529

Número de sequencias de tamanho 2:

0 = 1376

1 = 1295

Número de sequencias de tamanho 3:

0 = 733

1 = 655

Número de sequencias de tamanho 4:

0 = 238

1 = 354

Número de sequencias de tamanho 5:

0 = 94

1 = 200

Número de sequencias de tamanho 6+:

0 = 19

1 = 183

Chave Reprovada

- Chave 3

Número de sequencias de tamanho 1:

0 = 2863

1 = 2628

Número de sequencias de tamanho 2:

0 = 1346

1 = 1314

Número de sequencias de tamanho 3:

0 = 721

1 = 676

Número de sequencias de tamanho 4:

0 = 272

1 = 352

Número de sequencias de tamanho 5:

0 = 77

1 = 181

Número de sequencias de tamanho 6+:

0 = 23

1 = 150

Chave Reprovada

- Chave 4

Número de sequencias de tamanho 1:

0 = 2764

1 = 2640

Número de sequencias de tamanho 2:

0 = 1378

1 = 1322

Número de sequencias de tamanho 3:

0 = 719

1 = 601

Número de sequencias de tamanho 4:

0 = 291

1 = 361

Número de sequencias de tamanho 5:

0 = 88

1 = 167

Número de sequencias de tamanho 6+:

0 = 23

1 = 171

Chave Reprovada

- Chave 5

Número de sequencias de tamanho 1:

0 = 2674

1 = 2591

Número de sequencias de tamanho 2:

0 = 1419

1 = 1313

Número de sequencias de tamanho 3:

0 = 752

1 = 631

Número de sequencias de tamanho 4:

0 = 253

1 = 320

Número de sequencias de tamanho 5:

0 = 90

1 = 172

Número de sequencias de tamanho 6+:

0 = 25

1 = 185

Chave Reprovada

- Chave 6

Número de sequencias de tamanho 1:

0 = 2732

1 = 2636

Número de sequencias de tamanho 2:

0 = 1410

1 = 1322

Número de sequencias de tamanho 3:

0 = 724

1 = 612

Número de sequencias de tamanho 4:

0 = 263

1 = 344

Número de sequencias de tamanho 5:

0 = 99

1 = 161

Número de sequencias de tamanho 6+:

0 = 26

1 = 179

Chave Reprovada

- Chave 7

Número de sequencias de tamanho 1:

0 = 2726

1 = 2634

Número de sequencias de tamanho 2:

0 = 1374

1 = 1260

Número de sequencias de tamanho 3:

0 = 741

1 = 633

Número de sequencias de tamanho 4:

0 = 266

1 = 363

Número de sequencias de tamanho 5:

0 = 99

1 = 177

Número de sequencias de tamanho 6+:

0 = 31

1 = 170

Chave Reprovada

- Chave 8

Número de sequencias de tamanho 1:

0 = 2601

1 = 2510

Número de sequencias de tamanho 2:

0 = 1370

1 = 1254

Número de sequencias de tamanho 3:

0 = 778

1 = 663

Número de sequencias de tamanho 4:

0 = 271

1 = 331

Número de sequencias de tamanho 5:

0 = 97

1 = 202

Número de sequencias de tamanho 6+:

0 = 26

1 = 182

Chave Reprovada

- Chave 9

Número de sequencias de tamanho 1:

0 = 2780

1 = 2526

Número de sequencias de tamanho 2:

0 = 1421

1 = 1332

Número de sequencias de tamanho 3:

0 = 697

1 = 652

Número de sequencias de tamanho 4:

0 = 237

1 = 370

Número de sequencias de tamanho 5:

0 = 85

1 = 180

Número de sequencias de tamanho 6+:

0 = 22

1 = 181

Chave Reprovada

- Chave 10

Número de sequencias de tamanho 1:

0 = 2771

1 = 2553

Número de sequencias de tamanho 2:

0 = 1415

1 = 1317

Número de sequencias de tamanho 3:

0 = 693

1 = 694

Número de sequencias de tamanho 4:

0 = 283

1 = 361

Número de sequencias de tamanho 5:

0 = 79

1 = 184

Número de sequencias de tamanho 6+:

0 = 19

1 = 151

Chave Reprovada

Chave 11

Número de sequencias de tamanho 1:

0 = 2476

1 = 2504

Número de sequencias de tamanho 2:

0 = 1285

1 = 1246

Número de sequencias de tamanho 3:

0 = 629

1 = 635

Número de sequencias de tamanho 4:

0 = 328

1 = 308

Número de sequencias de tamanho 5:

0 = 160

1 = 163

Número de sequencias de tamanho 6+:

0 = 134

1 = 156

Chave Aprovada

- Chave 12

Número de sequencias de tamanho 1:

0 = 2643

1 = 2557

Número de sequencias de tamanho 2:

0 = 1265

1 = 1324

Número de sequencias de tamanho 3:

0 = 614

1 = 636

Número de sequencias de tamanho 4:

0 = 301

1 = 323

Número de sequencias de tamanho 5:

0 = 155

1 = 133

Número de sequencias de tamanho 6+:

0 = 136

1 = 141

Chave Aprovada

- Chave 13

Número de sequencias de tamanho 1:

0 = 2461

1 = 2449

Número de sequencias de tamanho 2:

0 = 1306

1 = 1294

Número de sequencias de tamanho 3:

0 = 630

1 = 664

Número de sequencias de tamanho 4:

0 = 302

1 = 322

Número de sequencias de tamanho 5:

0 = 157

1 = 138

Número de sequencias de tamanho 6+:

0 = 151

1 = 140

Chave Aprovada

- Chave 14

Número de sequencias de tamanho 1:

0 = 2488

1 = 2435

Número de sequencias de tamanho 2:

0 = 1253

1 = 1307

Número de sequencias de tamanho 3:

0 = 634

1 = 609

Número de sequencias de tamanho 4:

0 = 341

1 = 330

Número de sequencias de tamanho 5:

0 = 131

1 = 150

Número de sequencias de tamanho 6+:

0 = 146

1 = 162

Chave Aprovada

- Chave 15

Número de sequencias de tamanho 1:

0 = 2462

1 = 2478

Número de sequencias de tamanho 2:

0 = 1221

1 = 1249

Número de sequencias de tamanho 3:

0 = 600

1 = 615

Número de sequencias de tamanho 4:

0 = 329

1 = 302

Número de sequencias de tamanho 5:

0 = 163

1 = 143

Número de sequencias de tamanho 6+:

0 = 179

1 = 166

Chave Aprovada

- Chave 16

Número de sequencias de tamanho 1:

0 = 2564

1 = 2410

Número de sequencias de tamanho 2:

0 = 1215

1 = 1298

Número de sequencias de tamanho 3:

0 = 602

1 = 624

Número de sequencias de tamanho 4:

0 = 312

1 = 340

Número de sequencias de tamanho 5:

0 = 152

1 = 156

Número de sequencias de tamanho 6+:

0 = 149

1 = 165

Chave Aprovada

- Chave 17

Número de sequencias de tamanho 1:

0 = 2487

1 = 2479

Número de sequencias de tamanho 2:

0 = 1261

1 = 1260

Número de sequencias de tamanho 3:

0 = 607

1 = 605

Número de sequencias de tamanho 4:

0 = 297

1 = 305

Número de sequencias de tamanho 5:

0 = 182

1 = 184

Número de sequencias de tamanho 6+:

0 = 152

1 = 153

Chave Aprovada

- Chave 18

Número de sequencias de tamanho 1:

0 = 2427

1 = 2491

Número de sequencias de tamanho 2:

0 = 1274

1 = 1223

Número de sequencias de tamanho 3:

0 = 613

1 = 632

Número de sequencias de tamanho 4:

0 = 322

1 = 321

Número de sequencias de tamanho 5:

0 = 168

1 = 146

Número de sequencias de tamanho 6+:

0 = 165

1 = 155

Chave Aprovada

- Chave 19

Número de sequencias de tamanho 1:

0 = 2514

1 = 2531

Número de sequencias de tamanho 2:

0 = 1241

1 = 1219

Número de sequencias de tamanho 3:

0 = 666

1 = 627

Número de sequencias de tamanho 4:

0 = 322

1 = 342

Número de sequencias de tamanho 5:

0 = 138

1 = 144

Número de sequencias de tamanho 6+:

0 = 138

1 = 155

Chave Aprovada

- Chave 20

Número de sequencias de tamanho 1:

0 = 2489

1 = 2609

Número de sequencias de tamanho 2:

0 = 1241

1 = 1224

Número de sequencias de tamanho 3:

0 = 670

1 = 620

Número de sequencias de tamanho 4:

0 = 331

1 = 278

Número de sequencias de tamanho 5:

0 = 145

1 = 156

Número de sequencias de tamanho 6+:

0 = 158

1 = 147

Chave Aprovada

Teste Long Run

- Chave 1

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 2

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 3

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 4

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 5

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 6

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 7

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 8

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 9

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 10

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 11

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 12

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 13

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 14

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 15

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 16

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 17

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 18

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 19

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada

- Chave 20

Número de sequencias de tamanho 34+:

0 = 0

1 = 0

Chave Aprovada