



CC 8550 – Simulação e Teste de Software

Aula 02 – Geração de números aleatórios

Geração de Números Aleatórios



Tópicos da Aula:

- *Aspectos da Aleatoriedade*
- Onde e porque usar numeros aleatórios ?
- O que é aleatoriedade (*filosoficamente*)?
- O que são Numeros Aleatórios (*matematicamente*)?
- Numeros Aleatórios realmente existem ?
- *Medidas de* (não) aleatoriedade.

Geração de Números Aleatórios



- Como podemos obter verdadeiros números aleatórios?
- Fontes não-eletrônicas
- Fontes eletrônicas.
 - Circuitos simples para gerador de números aleatórios
 - Exemplos
 - Nos computadores
 - Sem HW extra
 - Com adição de HW

Utilização da aleatoriedade



- Filosofia
- Matemática
- Ciência da Computação
- Segurança da Informação
- Engenharia de Software
- Eletrônica
- Estatística
- Engenharia
- Física
- Lógica
- Economia
- Arte

Utilização da aleatoriedade ???



00101101001111000100001011000100111101110110100001010011000110010000101011100000010000000010110000010111011001011010000
10101101100101101111001000001100011101110001101111001101000011110010101011100100111011110001000111000011101110101011111
0100101100010100001110100111010011101010101011110100110010101110110101101110111100100011000111101101011010111010101010
00110100011010110110100101001110110100111010110010100010111000011010101001010001100001011000100100001010101001111011011
10000100101000000001111001011010110111000000100101011111010111100001010000100011110010100101011111000000011111011111
10011000100011001101001101100001001100000110101110111011110101010100001100000000111100010100000001001010100001011011101
01100110011110111010010100010001001000010111011000000100100110101111110011111001010101011100100000000110001110010000001
010111001101110001100111110000000011000011011110000000001000011110100101110110001101111111011100010011010101110010100
00001100011011100010000010100011101000100110101111101111000101001111011101111101011110001001110110101100011101010101110
0101100110111011101100000001011110001100001000010100100010111010000110100001111000101001100100110001110010011001110111
111000110011011001000101011001110101010011001101111000101111011101010100110110000100010110010000000010010010011011010
1101111000100011110100010100101101000000010100100010010011000011110100100111101010001100011101101110100111010010
00101011101010010000001000111001010100011101101010011100100110100100010101000010101110011100110101010000000111100100
111110110010100111101001011110000010010110110101001100010100101110000110111100001100110000100101100111001101100011010
001110000001000010001100111100010011000001001010010011101000101111101111000000101010111100000101010000110111001001001
011100011000011011111011111001100010111011111101111101101111011010000101001110010010010000100000010010010100010111110
0101111101010001110001100000110000100101101101111001000101000011001010000010111110111100101111011100001000111010100100
11011101001010001011101001010100011011000100011011010000010000001001010010001111101000000101110010010100101111110101111
11010101010110110011100110001100010101011000100000110001001110110100000110000111001111011011110101110111111010011100100
01110101111011110101110000100101000001011101101101110100000010010111111101001001111101001110001111001010000101111
1001100111001110110101011011101000110111000001010000101111100100110011101110101011010001111101111101101111011110101100
000111001101010000011111110111111001000111101001010110000010100001011101001111001110101101011100011001111011010
11110111100111110110111100001000000010111100011101111111101001010111101101101111010111001110011010111111011000100000010111
1010111111010101010111100011111001010011100101100000100000110101100100010001000101010001110011011000111001001000110110
11110000011100000100111001001101001111111001100000001100110110011001001111011110010001000110111011101

Tabelas de números aleatórios



- Tippett em 1927, com 41.600 dígitos gerados a partir de estatísticas obtidas em censos
- Kendall e Babington-Smith em 1939, com 100.000 dígitos, gerados a partir de um sistema mecânico, criado pelos próprios autores.
- Os esforços de tabulação praticamente se encerraram com a publicação, em 1955, da monumental tabela com um milhão de dígitos aleatórios da Rand Corporation obtidos a partir de uma roleta eletrônica, feita especialmente para este propósito.

Programas Geradores de Números Aleatórios *H*

- Um GNA, é um **programa computacional** que deve ser capaz de **gerar valores aleatórios independentes e uniformemente distribuídos** (isto é, todos com a mesma probabilidade de ocorrência) no intervalo de 0 a 1.
- A busca de bons algoritmos geradores de números aleatórios só se desenvolveu plenamente quando do advento dos primeiros computadores digitais.

Números Pseudo-Aleatórios



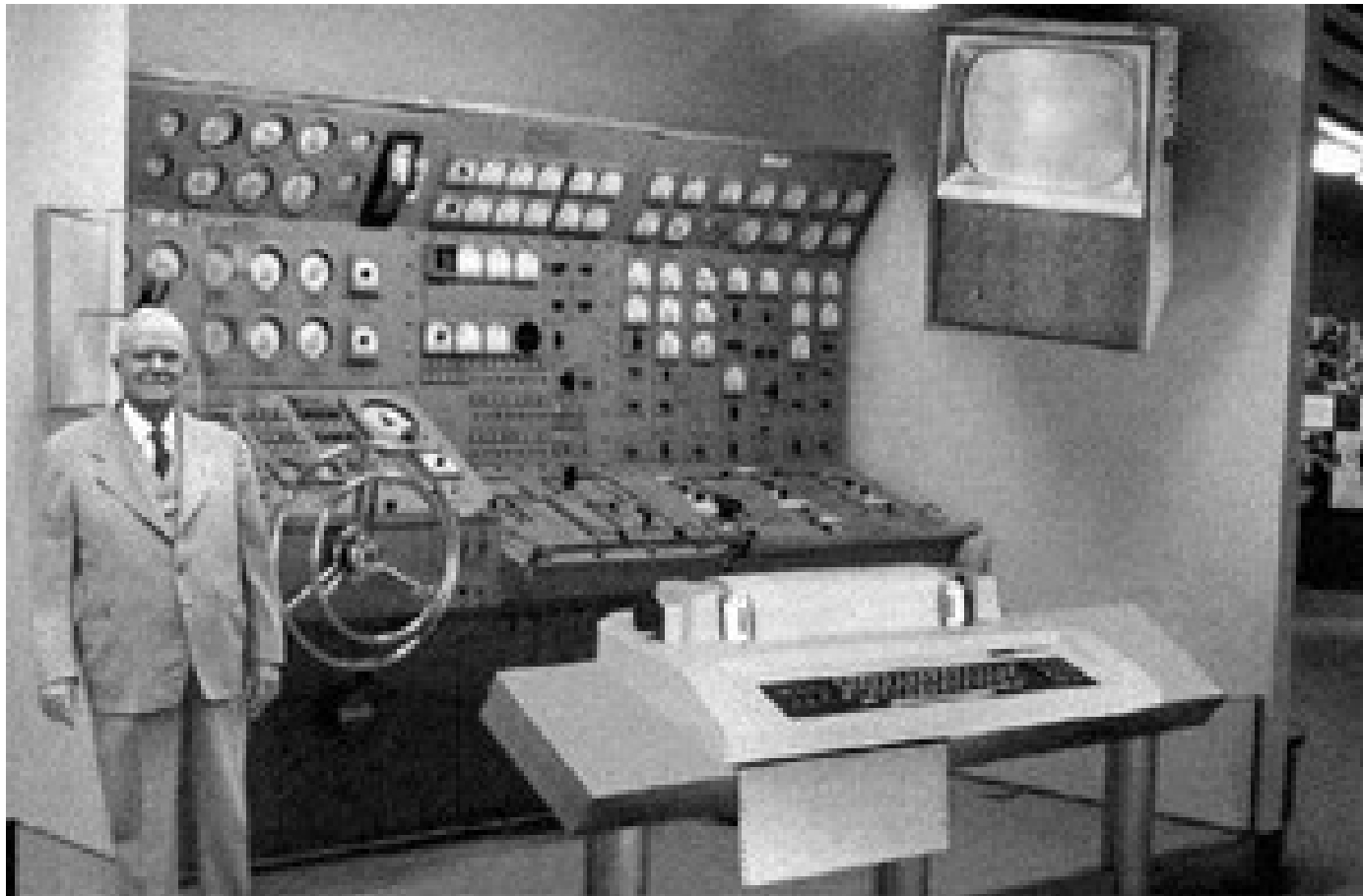
- Por serem gerados artificialmente, os valores aleatórios obtidos são conhecidos como números **pseudo-aleatórios**.
- Isto significa que a **seqüência** de números gerada por um destes algoritmos é **reproduzível** e, portanto, não aleatória no sentido estrito do termo.
- Estatisticamente falando, a comparação entre um conjunto de valores gerados em um computador com outro, verdadeiramente aleatório, gerado, por exemplo, pela natureza, **não apresenta diferenças**.
- E os números **VERDADEIRAMENTE** aleatórios?
- Você conhece algum **gerador natural**?

Tabela de Dígitos Aleatórios



2445	8615	2895	6331	5698	8294	1935	9192	4277	6365	1461	4693
8737	5112	3148	3470	1180	3662	5837	7458	7096	8545	2559	8704
8074	0700	8866	4050	5611	9691	7283	0279	0882	5464	2218	3014
8241	9290	3101	4657	8337	8247	1492	2507	1209	6216	3784	5015
6059	4324	0055	3590	7708	1107	8633	4402	8571	9892	9181	0602
0283	4899	2450	5647	7008	5411	5915	7467	4815	6311	4542	2468
6462	2135	7113	8994	2328	6156	7084	8395	4463	6345	9409	3804
2360	1613	4347	2364	9811	4581	5611	5835	2148	4565	0956	3918
0580	3417	6611	8927	3229	9247	4785	1877	5262	0646	8966	7341
6915	3167	5548	7352	3761	7086	0636	0079	0506	0718	1759	2979
8395	0617	4946	5390	8008	2785	7629	3176	5114	1410	0569	7877
3069	5769	3617	1149	0276	5783	2837	7487	8159	3478	8152	1191
1859	8790	3106	7156	5673	6967	0812	1603	1330	5588	3706	6479
9645	7574	2954	5940	6263	6559	9450	2281	1362	3000	0482	8066
1136	6008	0598	8617	2380	0960	4412	7829	2840	8729	4840	1130
4220	5296	9960	1179	9882	3223	7574	3009	0586	8087	9234	0536
2745	0643	5915	7618	4488	8871	4909	2972	6106	7307	5255	5101
2887	8586	0033	6146	6995	7415	9267	3306	4876	9378	0709	1284
1308	5453	4265	2823	3980	9271	7984	9418	1928	7429	9430	3280
5688	8902	6741	1182	5137	6712	3235	1171	7707	2947	3106	4346
7095	2239	2388	1595	4608	0700	2123	9659	1199	3279	5117	4105
4278	1820	8244	9860	1660	9044	8928	4588	1803	8097	9058	6465
1395	1223	7100	5349	2947	9933	9883	6823	5558	6412	5570	1611
3180	0778	4992	5550	0392	6390	7495	6931	7169	7232	3336	3652
3069	1381	0722	5843	1771	5534	5498	1546	5629	0224	6874	6951
4494	2202	2245	5608	3987	1528	3547	5980	9320	5533	8915	9216

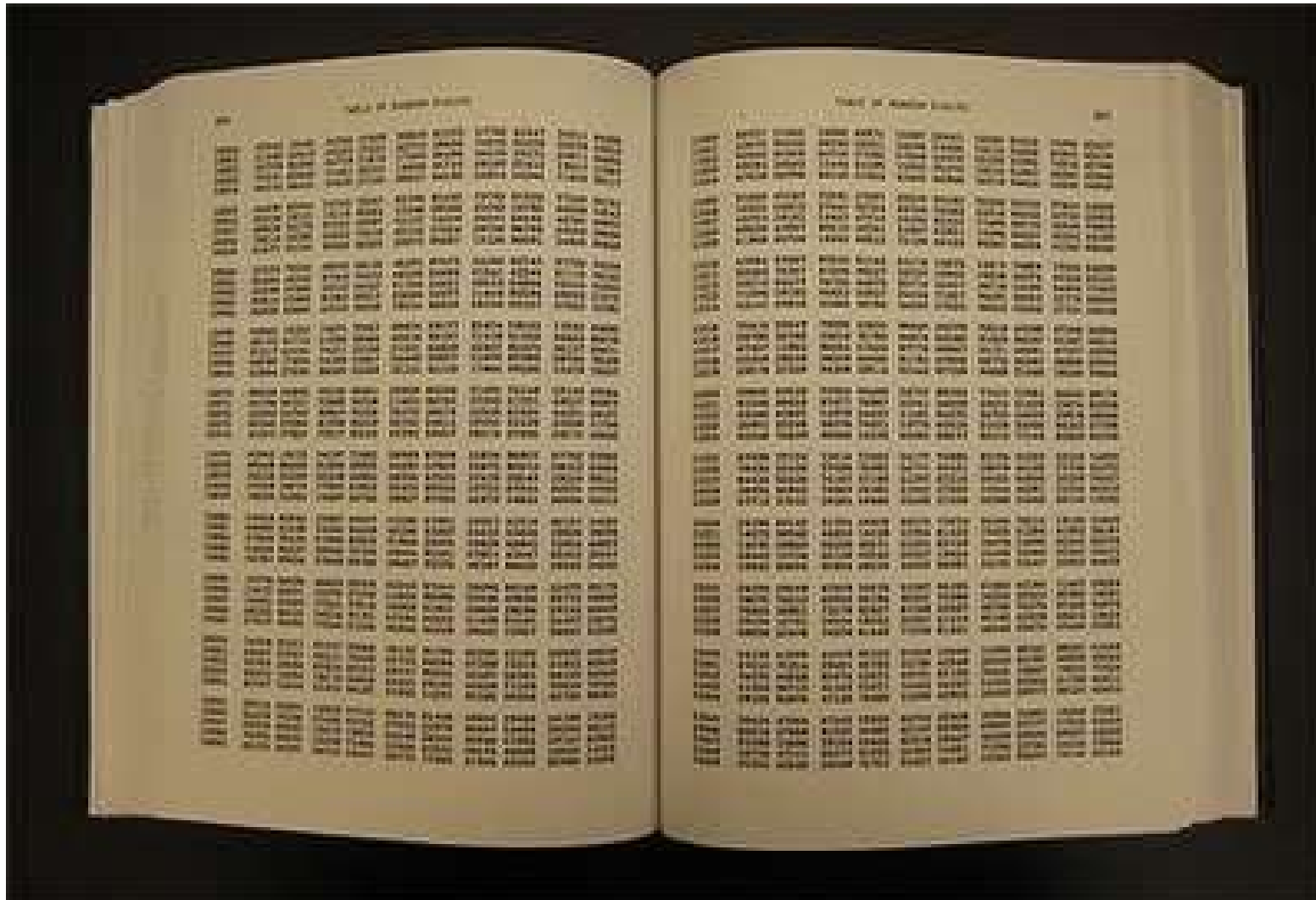
Tabela da Rand Corporation



Scientists from the RAND Corporation have created this model to illustrate how a "basic computer" could look like in the year 1964. However the needed technology will not be economically feasible for the average home. Also the scientists readily admit that the computer will require not yet invented technology to actually work, but 14 years from now scientific progress is expected to solve these problems. With teletype interface and the Fortran language, the computer will be easy to use.

Tabela da Rand Corporation

H



The image shows an open book displaying two pages of the Rand Corporation table. The pages are filled with a dense grid of numbers, organized into columns and rows. The text is printed in a small, serif font. The pages are slightly aged and the binding is visible in the center. The table is used for random sampling and is a key component of the RAND method for generating random numbers.

Números Aleatórios



É fácil gerar números aleatórios de cabeça?

- Cada pessoa pode anotar um número entre 0 e 100 em um pedaço de papel.
- Qual o número que mais ocorreu?



35

“Geradores de números aleatórios não devem ser escolhidos aleatoriamente” (Ronald Knuth)

17 é um número aleatório?

- $17 = 2^{2^2} + 1$
- 17 é sétimo número primo
- Podemos construir 17 gomos regulares com um compasso.

- Coincidência inédita na Mega-Sena provoca dúvidas nas redes sociais; matemáticos explicam
- Nathan Lopes Do UOL, em São Paulo
25/06/2018 13h09

Números Aleatórios



A Mega-Sena deste sábado (23) registrou pela primeira vez em 2.052 concursos, desde o lançamento da loteria em março de 1996, seis números da mesma dezena: 50 - 51 - 56 - 57 - 58 - 59. E, por mais improvável que essa combinação seja, teve gente que acreditou nela: quatro apostadores, das cidades de Salvador (BA), Maranguape (CE), Marabá (PA) e Canoas (RS), acertaram a sena.

As quatro apostas vencedoras dividirão um prêmio de R\$ 38.510.236,84, faturando R\$ 9.627.559,21 cada uma --o prêmio estava acumulado havia seis rodadas. O concurso 2.052 ocorreu às 20h (horário de Brasília), em Campina Grande (PB).

Números Aleatórios



Matematicamente, a chance de acertar as seis dezenas da Mega-Sena com um jogo simples é de uma em 50.063.860 possibilidades de combinações. Mas a aposta em seis números da mesma dezena chama ainda mais atenção por esse tipo de resultado nunca ter saído em nenhum dos 2.051 concursos anteriores ao deste sábado.

Apenas um concurso da Mega-Sena (o 1.004, de 13 de setembro de 2008) havia premiado mais de quatro números da mesma dezena, sorteando a combinação **29 - 40 - 43 - 44 - 45 - 47**. Na ocasião, ninguém acertou as seis dezenas e o prêmio de R\$ 10.552.054,80 foi acumulado para o sorteio seguinte.

Geração de Números Aleatórios



- Um número aleatório pode representar decisões arbitrárias ou servir como entrada para geração de tempos segundo várias distribuições.
- Como produzir números aleatórios ?
 - Dispositivos físicos (Ex. dados, roleta, moeda etc.)
 - Tabela de números aleatórios (livros)
 - Processos matemáticos
- No Excel: “=ALEATORIO()” (gera um número aleatório maior ou igual a 0 e menor do que 1)

Método do Meio Quadrado



- Von Neumann (1946)

- $r_1 = 76 \Rightarrow 76^2 = 5776$

- $r_2 = 77 \Rightarrow 77^2 = 5929$

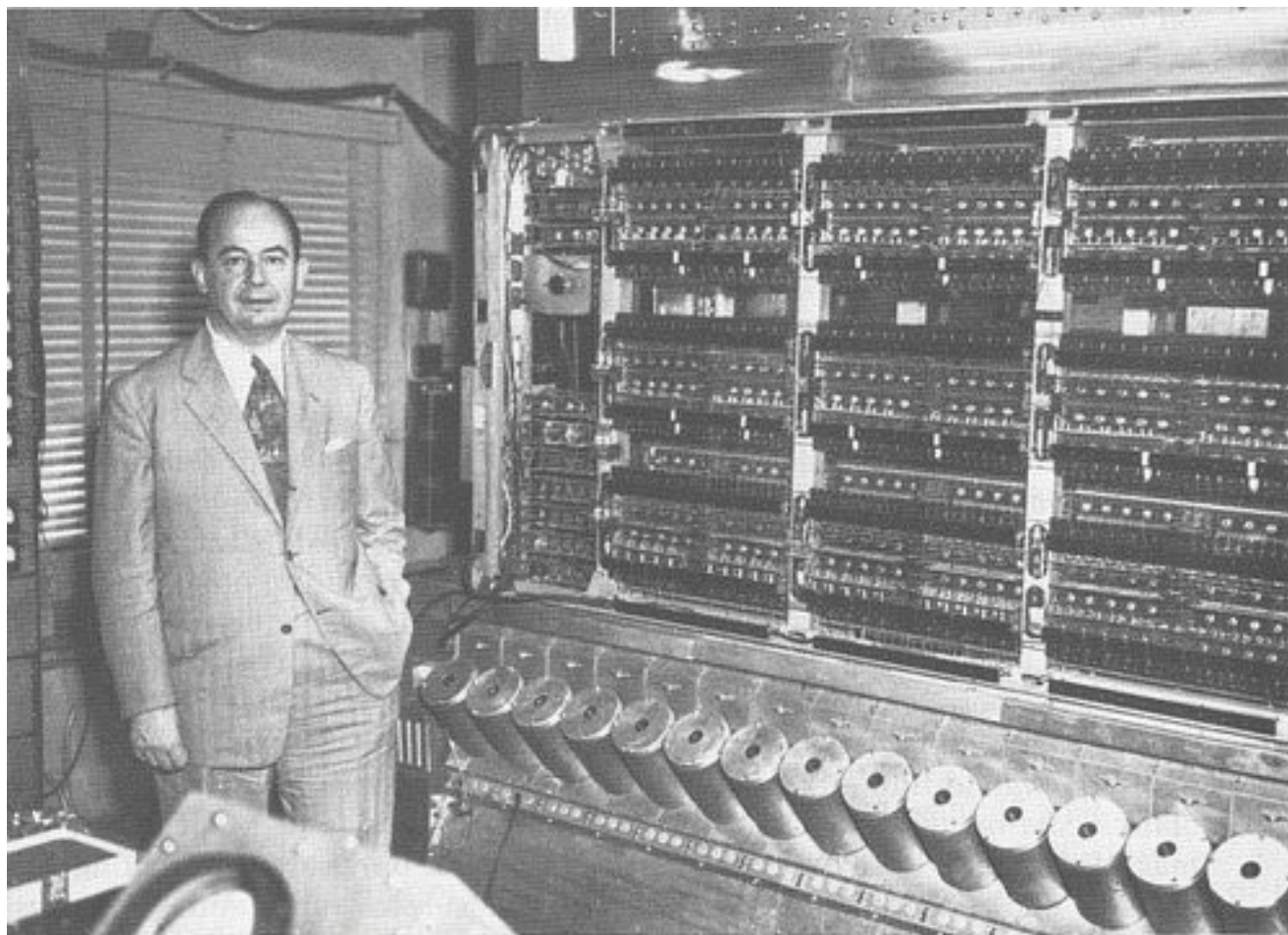
- $r_3 = 92....$



- Sequência gerada (76,77,92,46,11,12,14, ...)
- Quando resultar em 0, deve-se utilizar outra semente.

Método do Meio Quadrado

H



Método do Meio Quadrado – continuação *H*

$$x_0 = 5497$$

$$x_1: 5497^2 = 30\underline{2170}09 \rightarrow x_1 = 2170 \rightarrow R_1 = 0,2170$$

$$x_2: 2170^2 = 04\underline{7089}00 \rightarrow x_2 = 7089 \rightarrow R_2 = 0,7089$$

$$x_3: 7089^2 = 50\underline{2539}21 \rightarrow x_3 = 2539 \rightarrow R_3 = 0,2539$$

Desvantagem:

As condições de estado são difíceis para escolher a semente inicial que gerará uma sequência "boa".

Método do Meio Quadrado – continuação



Sequências “Ruins”

- $x_0 = 5197$

$$x_1: 5197^2 = 27\underline{0088}09 \rightarrow x_1 = 0088 \rightarrow R_1 = 0,0088$$

$$x_2: 0088^2 = 00\underline{0077}44 \rightarrow x_2 = 0077 \rightarrow R_2 = 0,0077$$

$$x_3: 0077^2 = 00\underline{0059}29 \rightarrow x_3 = 0059 \rightarrow R_3 = 0,0059$$

- $x_i = 6500$

$$x_{i+1}: 6500^2 = 42\underline{2500}00 \rightarrow x_{i+1} = 2500 \rightarrow R_{i+1} = 0,2500$$

$$x_{i+2}: 2500^2 = 06\underline{2500}00 \rightarrow x_{i+2} = 2500 \rightarrow R_{i+1} = 0,2500$$

Método do Meio Quadrado – continuação *H*

$$\begin{array}{rclclcl} x_0 & = & 121 & & & \\ (121)^2 & = & 014641 & \Rightarrow & x_1 & = & 464 \\ (464)^2 & = & 215296 & \Rightarrow & x_2 & = & 529 \\ (529)^2 & = & 279841 & \Rightarrow & x_3 & = & 984 \\ (984)^2 & = & 968256 & \Rightarrow & x_4 & = & 825 \\ (825)^2 & = & 680625 & \Rightarrow & x_5 & = & 062 \\ (062)^2 & = & 003844 & \Rightarrow & x_6 & = & 384 \\ (384)^2 & = & 147456 & \Rightarrow & x_7 & = & 745 \\ (745)^2 & = & 555025 & \Rightarrow & x_8 & = & 502 \\ (502)^2 & = & 252004 & \Rightarrow & x_9 & = & 200 \\ (200)^2 & = & 040000 & \Rightarrow & x_{10} & = & 000 \\ (000)^2 & = & 000000 & \Rightarrow & x_{11} & = & 000 \end{array}$$

Método da Congruência Linear (LCG)



$$x_{i+1} = (ax_i + c) \bmod m$$

*Gerador de números
inteiros entre 0 e m-1*

- “ x_0 ” é a semente do número aleatório
- “**mod**” é a função módulo = mostra o resto da divisão inteira.

Ex.: $10 \bmod 6 = 4$

Método da Congruência Linear (MCL)



Passo 1: *Escolher os valores a , c e M . Usualmente, M é escolhido o maior possível.*

Passo 2: *Escolher a semente r_0 , tal que: $1 \leq r_0 \leq M$.*

Passo 3: *Calcular o próximo número aleatório pela expressão:*

$$r_1 = (a \cdot r_0 + c) \bmod M$$

*onde: $x \bmod y$ é o módulo da divisão de x por y (por exemplo:
 $10 \bmod 6 = 4$).*

Passo 4: *Substitua r_0 por r_1 e volte ao passo anterior, de modo a construir a seqüência de números aleatórios desejada.*

Método da Congruência Linear (MCL)

Gerar números aleatórios pelo método da congruência,
com $a = 9$, $c = 1$, $m = 17$ e $x_0 = 7$.

n	x_n	$y=9x_n+1$	$y \bmod 17$	$x_{n+1}/17$
0	$x_0=7$	$9*7+1=64$	13	$13/17 = 0.7647$
1	$x_1=13$	118	16	$16/17 = 0.9412$
2	$x_2=16$	145	9	0.5294
3	$x_3=9$	82	14	0.8235
4	$x_4=14$	127	8	0.4706

*números pseudo-aleatórios
inteiros entre 0 e 16 (=17-1)*

*números pseudo-aleatórios inteiros
entre 0 e 1*

Exemplo 01



X	X - Norm
27	0.27
2	0.02
77	0.77
52	0.52
27	0.27
2	0.02
77	0.77
52	0.52
27	0.27
2	0.02
77	0.77
52	0.52
27	0.27

$$X_{i+1} = (aX_i + c) \bmod m, \quad i = 0, 1, 2, \dots$$

O ciclo é tamanho 4.

Isso é aceitável ?

$X_0 = 27$, $a = 17$, $c = 43$, $m = 100$,

$$0 \leq X \leq 99$$

O que acontece se for usada uma semente diferente ?

Exemplo 02 – Usando uma semente diferente *H*

$$X0 = 3$$

$$a = 17$$

$$c = 43$$

$$m=100$$

Agora o comprimento do ciclo é de 20

Obs:

1. Os dois ciclos são pequenos
2. O tamanho do ciclo depende da escolha da semente

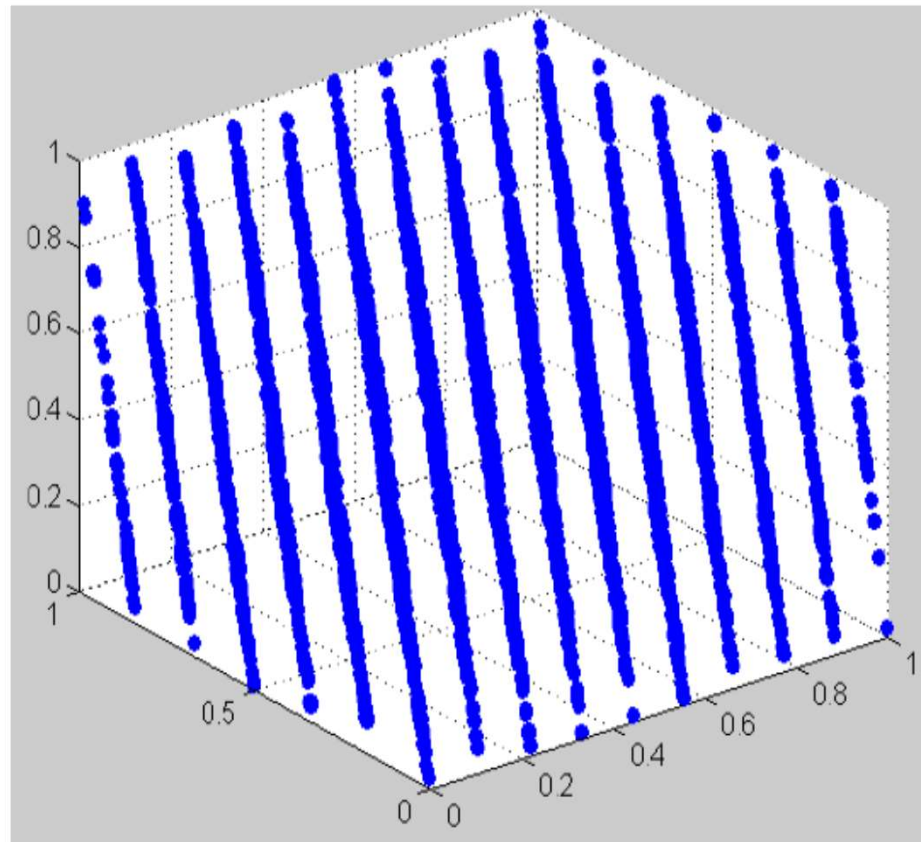
3	0.03
94	0.94
41	0.41
40	0.4
23	0.23
34	0.34
21	0.21
0	0
43	0.43
74	0.74
1	0.01
60	0.6
63	0.63
14	0.14
81	0.81
20	0.2
83	0.83
54	0.54
61	0.61
80	0.8
3	0.03
94	0.94

Uso do MCL



Implementação	a	b	c	S_1
IBM RANDU	65539	0	2^{31}	123456789
Congruência Linear mínima	16807	0	$2^{31} - 1$	1
função rand() linguagem C (ANSI)	1103515245	12345	2^{31}	12345
Numerical Recipes	1664525	1013904223	2^{32}	1
CRAY	44485709377909	0	2^{48}	1
Maple	427419669081	0	$10^{12} - 11$	1

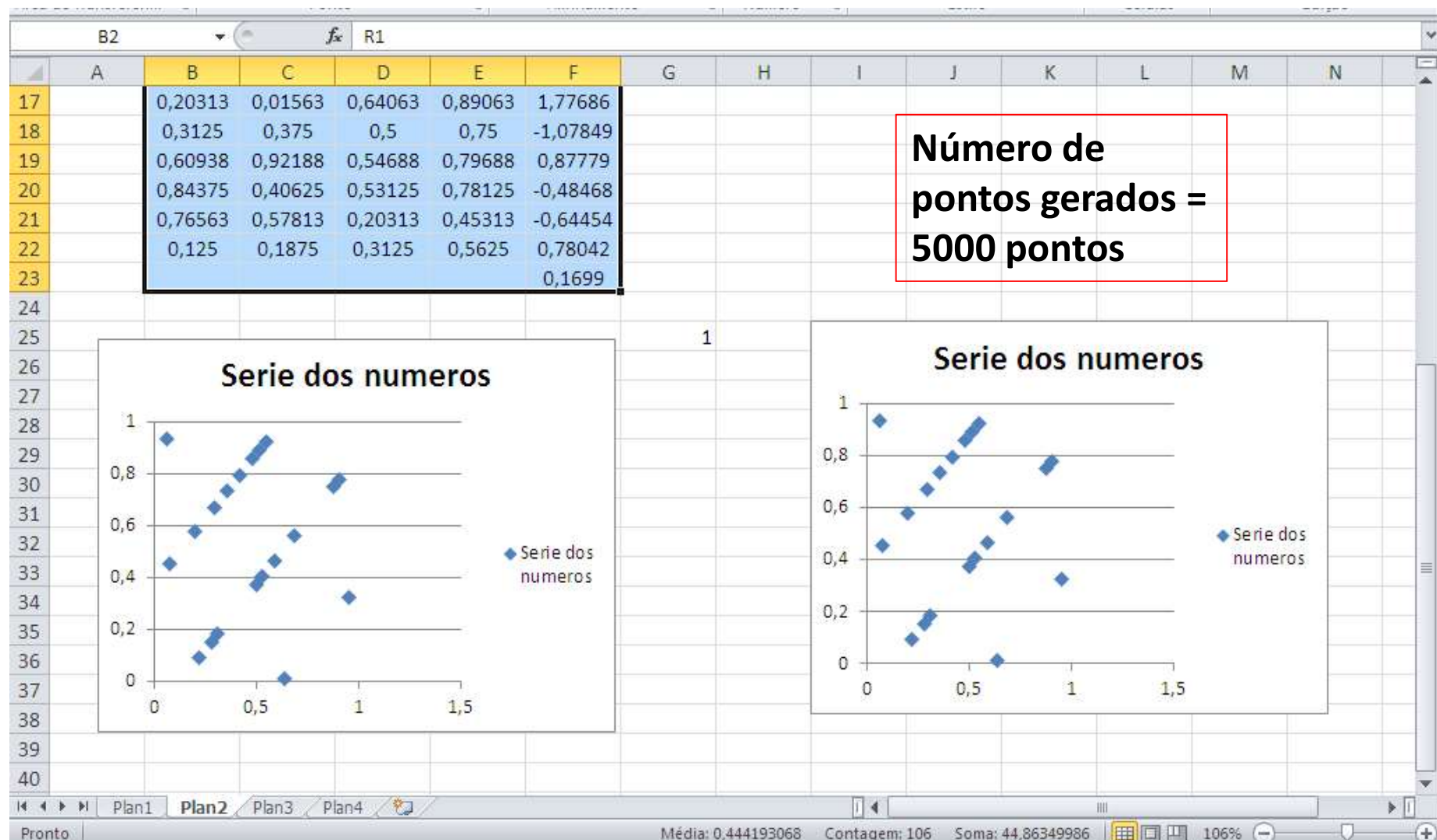
Gráfico do Gerador RANDU (cubo com coordenadas) *H*



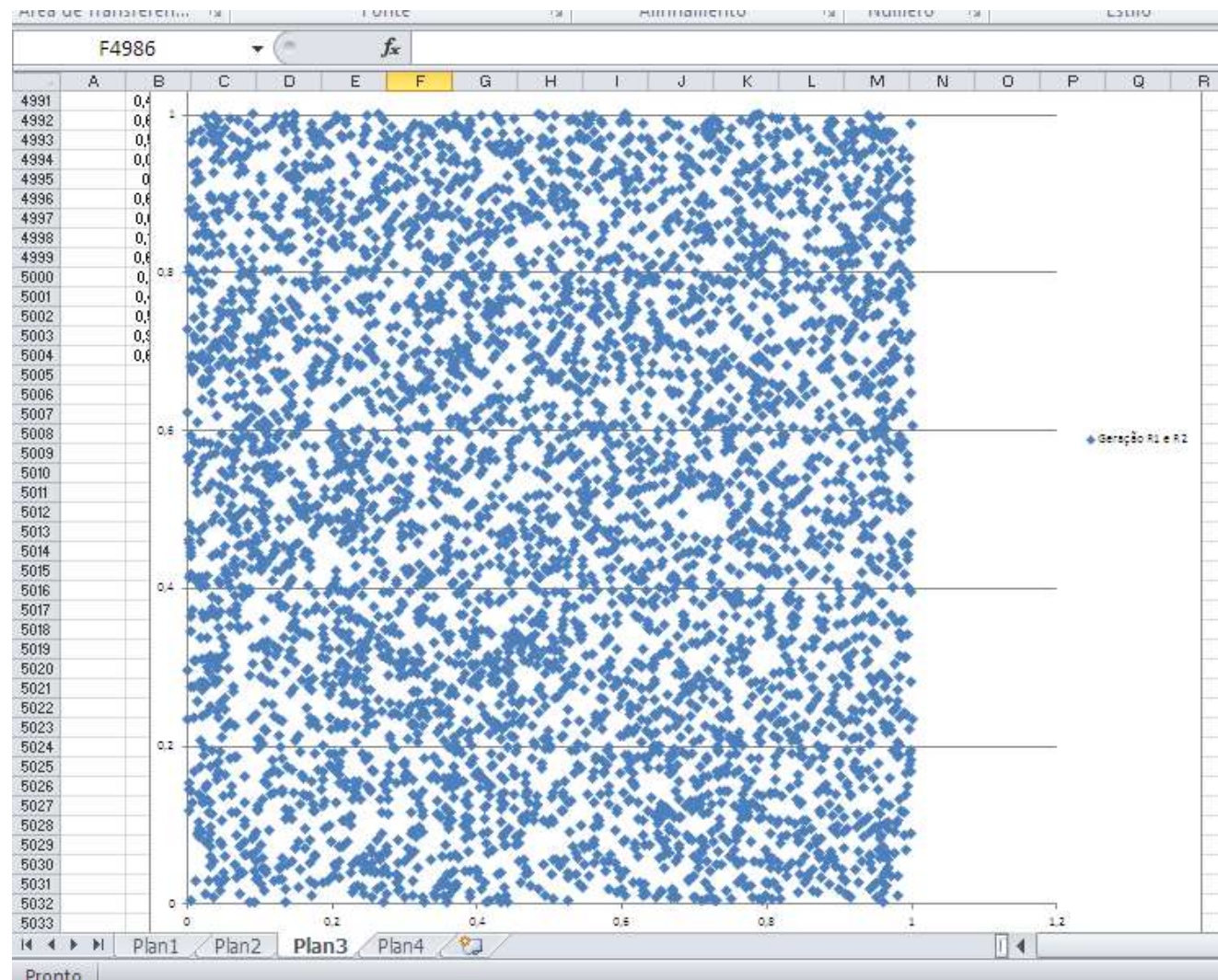
Número de
pontos gerados =
5000 pontos

Figura 01: Imagem tridimensional correspondente a 5.000 pontos gerados a partir da Implementação RANDU. Os pontos ocupam apenas 15 planos contidos no cubo! Um péssimo comportamento “aleatório”.

Verificação da geração com um número de Matricula *H*



Geração de números aleatórios no Excel



**Número de
pontos gerados =
5000 pontos**

Geração de Números Aleatórios

H



RSA SecurID SD600



RSA SecurID SID700



RSA SecurID SD200



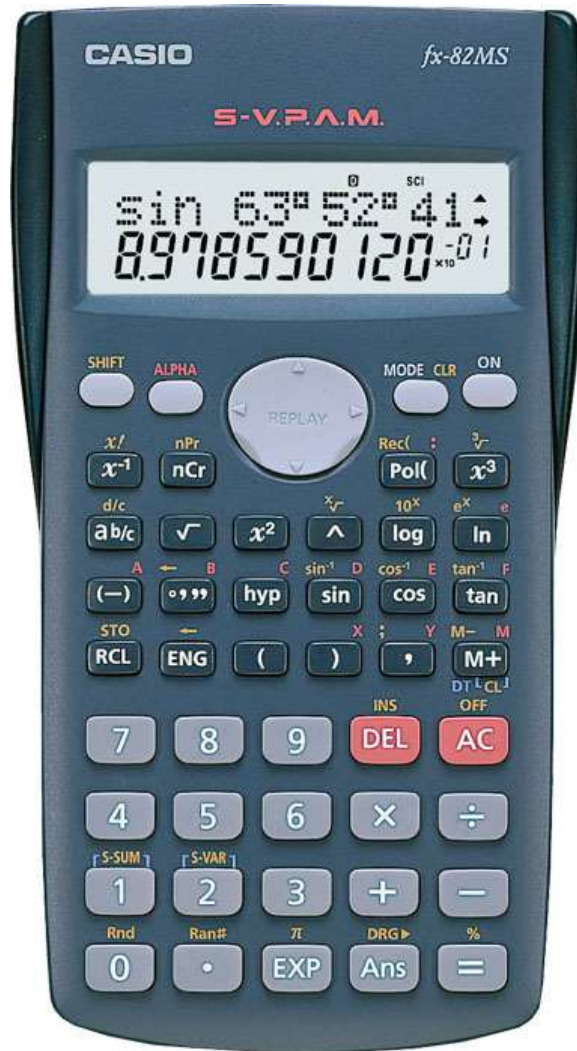
RSA SecurID SID800



RSA SecurID SD520

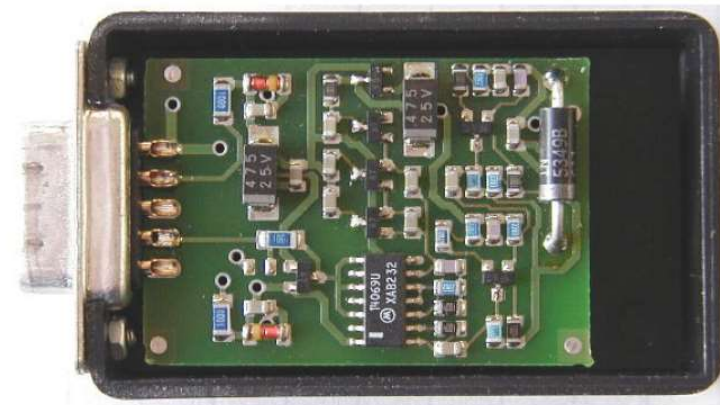


Geradores de Números Aleatórios



Geração de Números Aleatórios

H



Geração de Números Aleatórios



Geração de Números Aleatórios



Galaxy Note20 | 20 Ultra 5G

Pré-venda

03.09 a 17.09

Compre um Galaxy Note20
ou Note20 Ultra e
ganhe um voucher

Home > Produtos > Smartphone

**Samsung anuncia o Galaxy A Quantum com gerador
quântico de números aleatórios**

Por Rubens Eishima | 14 de Maio de 2020 às 09h00

 5K Telecom

Geração de Números Aleatórios



A [Samsung](#) anunciou o lançamento de um modelo exclusivo para a operadora SK Telecom, na Coreia do Sul. Trata-se do Galaxy A Quantum, versão especial do [Galaxy A71 5G](#) equipada com um gerador quântico de números aleatórios (QRNG, na sigla em inglês).

O aparelho segue as [especificações originais da versão 5G](#) do [Galaxy A71](#), com a inclusão do processador IDQ250C2, desenvolvido pela SK Telecom com tecnologias licenciadas da suíça [ID Quantique](#).

- [Mozilla vai implementar gerador aleatório de senhas no Firefox](#)
- [Cientistas criam método para criptografar informações por meio de cristais](#)

QRNG?

Segundo as empresas envolvidas, o uso do gerador serve para aumentar a segurança dos dados armazenados no aparelho. O processador pode ser usado para gerar senhas criptografadas realmente aleatórias em vez de se basear em informações como hora e



Pré-venda | 03.09 a 17.09

Compre um Galaxy Note20 ou Note20 Ultra e
ganhe um voucher de R\$ 2.000
para comprar mais produtos da linha Galaxy.

Geração de Números Aleatórios



- Cientistas criam método para criptografar informações por meio de cristais

QRNG?

Segundo as empresas envolvidas, o uso do gerador serve para aumentar a segurança dos dados armazenados no aparelho. O processador pode ser usado para gerar senhas criptografadas realmente aleatórias em vez de se basear em informações como hora e data, aumentando a imprevisibilidade da combinação utilizada.

Processadores comuns encontrados em celulares possuem geradores de números aleatórios, mas eles se baseiam em um valor inicial, conhecido como “semente”, o que faz com que sejam chamados de **geradores pseudo-aleatórios**.

CONTINUA DEPOIS DA PUBLICIDADE



SAMSUNG

Galaxy Note20 | 20 Ultra 5G

Pré-venda
03.09 a 17.09

Compre um Galaxy Note20
ou Note20 Ultra e
**ganhe um voucher
de R\$ 2.000**

/click?xai=AKAOjstz0KbmnbLZSw7vCpEz3SbmWKL7try5Wcz28Bk-Zlui_DOT1-l-mhyyWPYDW-2KA0-hzvTwSQuDnrv7GQuSKIsAFGS1jxVznZDqL9FSDpbu0yLtlj3fvmHqR4ZpNs_aoYr4SV

Geração de Números Aleatórios



Os valores gerados podem ser usados, por exemplo, para criar o código que protege as comunicações feitas pelo [WhatsApp](#) – a [criptografia](#) ponta a ponta que o app menciona. Outras aplicações do gerador estão na proteção de conexões seguras, pagamentos com o celular por aproximação ([NFC](#)) e [geração de códigos de autenticação](#).



Geração de Números Aleatórios



Gerador quântico indica 2,5 milímetros de largura no paquímetro (imagem: SK Telecom)

Geração de Números Aleatórios



Gerador quântico indica 2,5 milímetros de largura no paquímetro (imagem: SK Telecom)

Especificações

- Tela: 6,7 polegadas, Super AMOLED, Full HD+
- Chipset: Exynos 980
- Memória RAM: 8 GB
- Armazenamento interno: 128 GB
- Câmera traseira: 64 (principal) + 12 (ultrawide) + 5 (macro) + 5 MP (sensor de profundidade)
- Câmera frontal: 32 megapixels
- Bateria: 4.500 mAh, recarga a 25 W
- Extras: 5G, NFC, gerador quântico de números aleatórios
- Cores disponíveis:
- Sistema operacional: Android 10 com personalização One UI 2.0

Fonte: [ID Quantique](#)