РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

Бұдан қандай да бір k нөмірден бастап барлық φ_i функциялары нөлге айналатындығы көрініп тұр. Демек (11) формуламен анықталатын функцияға қатысатын $\varphi_i(x)\ \left(i=\overline{1,m}\right)$ функцияларын $u(x,t)$ функциясы (7)-(8) есебінің шешімі болатындай етіп таңдап алуға болады.Сондықтан $u(x,t)$ функциясы (7)-(8) есебінің дербес шешімін анықтайды.

Салдар 1. $f(x,t)=g(x)$ болсын. Егер $\Delta^n g=0,\ \ \Delta^n u_0(x)=0$ болатындай $n\in N$ нөмірі табылатын болса, онда

$$u(x,t)=u_0(x)+t\varphi_1(x)+\frac{t^2}{2!}\varphi_2(x)+\ldots+\frac{t^m}{m!}\varphi_m(x)$$

функция (9)-(10) есебінің дербес шешімін анықтайды.

Ескерту2. Егер $u_0(x),\ u_1(x)$ функциялары жоғарыдағы шарттарды қанағаттандырмайтын болса,онда дербес шешімді

$$u(x,t)=\frac{t^2}{2!}\varphi_2(x)+\ldots+\frac{t^m}{m!}\varphi_{m-1}(x)$$

түрінде іздестірген өте ыңғайлы.

Ескерту3. Біртекті толқын және жылуөткізгіштік теңдеулердің $m>1$ болғанда жалпы шешімі болмайтын болғандықтан, дербес шешімді тапқаннан кейін теңдеу біртекті болатындай

$$\vartheta(x,t)=u(x,t)-u_{дербес}(x,t)$$

жылжыту жасау қажет.

Қолданылған әдебиеттер тізімі

1. Владимиров В.С. Уравнения математической физики.-М.:Наука,1988.
2. Уроев В.М. Уравнения математической физики.-М.:ИФ Яуза,1998.
3. Владимиров В.С., Вашарин А.А., Каримова Х.Х., Михайлов В.П., Сидоров Ю.В., Шабунин М.И. Сборник задач по уравнениям математической физики. - М.: Физматлит,2004.
4. Кузнецов Е.А,. Шапиро Д.А. Методы математической физики. - М.: Новосибирск 2011.

УДК: 519.246

ПРИМЕНЕНИЕ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ ЛЕХМЕРА В КРИПТОГРАФИИ

Әскербеков Мейіржан Әскербекұлы

meirzhan-250@mail.ru

Магистрант Института теоретической математики
и научных вычислений ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – М.Жайнибекова

Статья посвящена получению случайных чисел с использованием генератора случайных чисел Лехмера. Цель работы – построение случайной линейной конгруэнтной последовательности с максимальным периодом (определение см. ниже) и их практическое применение в задачах криптографии.

Случайные числа имеют большое количество приложений в различных областях человеческой деятельности: в криптографии, в вычислениях, в моделировании, в промышленных испытаниях, в азартных играх и т.д.

Согласно [1, стр. 4]: «*Криптография — это наука о способах преобразования информации и данных с целью их защиты от незаконных пользователей.*

Несмотря на многочисленные применения случайных чисел нет их единого определения. Здесь приведем несколько примеров определений случайных чисел из различных источников.

Определение 1 [2, стр. 167]. *Случайная последовательность является смутным понятием, олицетворяющим идею последовательности, в которой каждый член является непредсказуемым для непосвященных. А также значения, которых проходят определенное количество проверок, традиционных у статистиков и отчасти зависящих от пользователей, которым предложена последовательность.*

Определение 2 [3, стр. 176]. *С неформальной точки зрения случайность можно определить как непредсказуемость значений данных для злоумышленника, даже если тот предпримет активные шаги для борьбы со случайностью.*

Определение 3 [4]. *Случайное число это число, выбранное, как будто случайно из некоторого заданного распределения таким образом, что выбор больших наборов этих чисел воспроизводит основное распределение. Почти всегда, такие числа также должны быть независимыми, так что нет корреляции между последовательными номерами. Компьютерные генерируемые случайные числа иногда называют псевдослучайных чисел, в то время как термин "случайный" зарезервирован для выхода непредсказуемых физических процессов. При использовании без квалификации, слово "случайный" обычно означает "случайный с равномерным распределением." Другие дистрибутивы, конечно, можно.*

Генератор псевдослучайных чисел (ГПСЧ) [5] — алгоритм, генерирующий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению.

Современная криптография обширно использует псевдослучайные числа в самых различных приложениях. Тем самым задача построения случайных чисел является актуальной.

В работе [2, стр. 29]: «*В настоящее время наиболее популярными генераторами случайных чисел являются генераторы, в которых используется следующая схема, предложенная Д.Г.Лехмером (D.H.Lehmer) в 1949 году. Выберем четыре "волшебных числа":*

N, *модуль* $0 < N$

a, *множитель* $0 \le a < N$

c, *приращение* $0 \le c < N$

X_0, *начальное значение* $0 \le X_0 < N$

Затем получим желаемую последовательность случайных чисел $\{X_n\}$, *полагая*

$$X_{n+1} = (aX_n + c) \bmod N \ (n = 0,1,...,N). \qquad (1)$$

Эта последовательность называется ***линейной конгруэнтной последовательностью».***

В 1965г. Р. Ковэю и Р. Макферсоном построен спектральный тест проверки линейных конгруэнтных последовательностей на случайность [6, стр. 105], где в качестве меры «случайности» линейных конгруэнтных последовательностей (1) с множителем a и максимальным периодом N принимается величина:

$$\nu_s(a,N) = \min_{\substack{(m_1,...,m_s)\in Z^s \\ (m_1,...,m_s)\neq(0,0,...,0): \\ m_1+am_2+...+a^{s-1}m_s\equiv 0 (\bmod N)}} \sqrt{m_1^2+...+m_s^2}\ .$$

В [7, стр 71] дано правило построения генераторов случайных чисел $\{X_n(a,N)\}$ с максимальным периодом: Если при данном $s, s \ge 2$ требуется построить генератор с наибольшим $\nu_s(a,N)$, то a и N, $a < N$ должны быть связаны равенством $(a-1)^s = N$.

Пусть «Mersin University» текст, который необходимо зашифровать. Данный текст состоит из $m = 16$ символов.

Построим две последовательности случайных чисел на основе правила данного в [7, стр 71]. Первую последовательность с длиной N_1, а вторую с длиной $N_2 \geq N_1 + m = N_1 + 16$. Для первой последовательности $a_1 = 17, s = 2$ и $N_1 = 256$:

$$X_{n+1} = (a_1 X_n + 1) \bmod N_1 = (17 \cdot X_n + 1) \bmod 256, \ (n = 0,...,255 ; X_0 = 0).$$

Таблица 1.

Последовательность случайных чисел $\{X_n\}_{n=0}^{255}$.

0	1	18	51	100	165	246	87	200	73	218	123	44	237	190	159	144	145	162	195	244
53	134	231	88	217	106	11	133	125	78	47	32	33	50	83	132	197	22	119	232	105	250
155	76	13	222	191	176	177	194	227	20	85	166	7	120	249	138	43	220	157	110	79
64	65	82	115	164	229	54	151	8	137	26	187	108	45	254	223	208	209	226	3	52	117
198	39	152	25	170	75	252	189	142	111	96	97	114	147	196	5	86	183	40	169	58	219
140	77	30	255	240	241	2	35	84	149	230	71	184	57	202	107	28	221	174	143	128
129	146	179	228	37	118	215	72	201	90	251	172	109	62	31	16	17	34	67	116	181	6
103	216	89	234	139	60	253	206	175	160	161	178	211	4	69	150	247	104	233	122	27
204	141	94	63	48	49	66	99	148	213	38	135	248	121	10	171	92	29	238	207	192	193
210	243	36	101	182	23	136	9	154	59	236	173	126	95	80	81	98	131	180	245	70	167
24	153	42	203	124	61	14	239	224	225	242	19	68	133	214	55	168	41	186	91	12	205
158	127	112	113	130	163	212	21	102	199	56	185	74	235	156	93	46	15				

Теперь построим вторую последовательность $\{Y_n\}_{n=0}^{840}$ по $a_2 = 30, s = 2$, $(a-1)^s = N_2$

$$Y_{n+1} = (a_2 \cdot Y_n + 1) \bmod N_2 = (30 \cdot Y_n + 1) \bmod 841, \ (n = 0,...,840; Y_0 = 0).$$

Таблица 2.

Последовательность случайных чисел $\{Y_n\}_{n=0}^{840}$.

1	31	90	178	295	441	616	820	212	474	765	244	593	130	537	132	597	250	773	484	
224	834	632	459	315	200	114	57	29	30	60	119	207	324	470	645	8	241	503	794	273
622	159	566	161	626	279	802	513	253	22	661	488	344	229	143	86	58	59			
89	148	236	353	499	674	37	270	532	823	302	651	188	595	190	655	308	831	542	282	
51	690	517	373	258	172	115	87	88	118	177	265	382	528	703	66	299	561			
11	331	680	217	627	219	684	337	19	571	311										
80	719	546	402	287	201	144	116	147	206	294	411	557	732	95	328	590				
40	360	709	246	653	248	713	366	48	600	340	109	748	575	431	316	230	173			
145	146	176	235	323	440	586	761	124	357	619	69	389	738	275	682	275	682	277	742	395
77	629	369	138	777	604	460	345	259	202	174	175	205	264	352	469	615	790	153	386	648
98	418	767	304	711	306	771	424	106	658	398	167	806	633	489	374	288	231	203	204	
234	293	381	498	644	819	182	415	677	127	447	796	333	740	335	800	453	135	687	427	196
835	662	518	403	317	260	232	233	263	322	410	527	673								
7	211	444	706	156	476	825	362	769	364	829	482	164	716	456	225					
23	691	547	432	346	289	261	262	292	351	439	556	702	36	240	473	735	185	505		
13	391	798	393	17	511	193	745	485	254											
52	720	576	461	375	318	290	291	321	380	468	585	731	65	269	502	764	214	534		
42	420	827	422	46	540	222	774	514	283											
81	749	605	490	404	347	319	320	350	409	497	614	760	94	298	531	793	243	563	71	449
15	451																			
75	569	251	803	543	312	110	778	634	519	433	376	348	349	379	438	526	643	789	123	327	56
0	822	272	592	100	478															
44	480	104	598	280	832	572	341	139	807	663	548	462	405	377	378	408	467	555	672	818	1

52 356 589 10 301 621 129 507 73 509 133 627 309
20 601 370 168 836 692 577 491 434 406 407 437 496 584 701 6 181 385 618
39 330 650 158 536 102 538 162 656 338 49 630 399 197
24 721 606 520 463 435 436 466 525 613 730 35 210 414 647 68 359
679 187 565 131 567 191 685 367 78 659 428 226 53 750 635 549 492
464 465 495 554 642 759 64 239 443 676
97 388 708 216 594 160 596 220 714 396 107 688 457 255
82 779 664 578 521 493 494 524 583 671 788 93 268
472 705 126 417 737 245 623 189 625 249 743 425 136 717 486 284 111 808 693 607 55
0 522 523 553 612 700 817 122 297 501 734 155 446 766 274 652 218 654 278
772 454 165 746 515 313 140 837 722 636 579 551 552 582 641 729
5 151 326 530 763 184 475 795 303 681 247 683 307 801 483 194 775 544 342 169
25 751 665 608 580 581 611 670 758 34 180 355 559 792 213
504 824 332 710 276 712 336 830 512 223 804 573 371 198
54 780 694 637 609 610 640 699 787 63 209 384 588 821 242 533 12
361 739 305 741 365 18 541 252 833 602 400 227 83 809 723 666 638 639 669 728 816
92 238 413 617 9 271 562 41 390 768 334 770 394 47 570 281 21 631 429
256 112 838 752 695 667 668 698 757 4 121 267 442 646 38 300 591
70 419 797 363 799 423 76 599 310 50 660 458 285 141 26 781 724 696 697 727 786
33 150 296 471 675 67 329 620 99 448 826 392 828 452 105 628 339
79 389 487 314 170 55 810 753 725 726 756 815 62 179 325 500 704 96 358 649 128 477
14 421 16 481 134 657 368 108 718 516 343 199 84 839 782 754 755 785 3 91 208 354
529 733 125 387 678 157 506 43 450 45 510 163 686 397 137 747 545 372 228 113
27 811 783 784 814 32 120 237 383 558 762 154 416 707 186 535 72 479
74 539 192 715 426 166 776 574 401 257 142 56 840 812 813 2
61 149 266 412 587 791 183 445 736 215 564 101 508 103 568 221 744 455 195
805 603 430 286 171 85 28

Таблица 3.

Пронумеруем буквы английского алфавита:

№	буква	№	буква
0	A a	13	N n
1	B b	14	O o
2	C c	15	P p
3	D d	16	Q q
4	E e	17	R r
5	F f	18	S s
6	G g	19	T t
7	H h	20	U u
8	I i	21	V v
9	J j	22	W w
10	K k	23	X x
11	L l	24	Y y
12	M m	25	Z z

К каждой букве данного текста поставим в соответствие порядковые номера с Таблицы 3. Тогда имеем слудующую конечную последовательность чисел

12 4 17 18 8 13 20 13 8 21 4 17 18 8 19 24.

Таким образом, получаем 16 символов $t_1 = 12, t_2 = 4, ..., t_{16} = 24.$

В алгоритме шифрования нашего текста будем использовать две последовательности $\{X_n\}_{n=0}^{255}$ и $\{Y_n\}_{n=0}^{840}$. Выберем случайное число K из множества $\{0,1,2,...,255\}$. Например K=7. Данному K поставим в соответствие X_K. Тогда $K=7 \to X_K = X_7 = 87$. Числу 87 поставим в соответствие конечную последовательность $Y_{X_K}, Y_{X_K+1,...,} Y_{X_K+m-1}$, т.е. $Y_{87}, Y_{88,...,} Y_{102}$. Обозначим $\tau_1 = Y_{X_K}, \tau_2 = Y_{X_K+1}, ..., \tau_m = Y_{X_K+m-1}$.

Зашифруем текст «Mersin University» по формуле $\theta_i = t_i + \tau_i (\mathrm{mod}\, N_2)$.

$\theta_1 = 12 + 87 (\mathrm{mod}\, 841) = 99$ $\theta_9 = 8 + 66 (\mathrm{mod}\, 841) = 74$

$\theta_2 = 4 + 88 (\mathrm{mod}\, 841) = 92$ $\theta_{10} = 21 + 299 (\mathrm{mod}\, 841) = 320$

$\theta_3 = 17 + 118 (\mathrm{mod}\, 841) = 135$ $\theta_{11} = 4 + 561 (\mathrm{mod}\, 841) = 565$

$\theta_4 = 18 + 177 (\mathrm{mod}\, 841) = 195$ $\theta_{12} = 17 + 11 (\mathrm{mod}\, 841) = 28$

$\theta_5 = 8 + 265 (\mathrm{mod}\, 841) = 273$ $\theta_{13} = 18 + 331 (\mathrm{mod}\, 841) = 349$

$\theta_6 = 13 + 382 (\mathrm{mod}\, 841) = 395$ $\theta_{14} = 8 + 680 (\mathrm{mod}\, 841) = 688$

$\theta_7 = 20 + 528 (\mathrm{mod}\, 841) = 548$ $\theta_{15} = 19 + 217 (\mathrm{mod}\, 841) = 236$

$\theta_8 = 13 + 703 (\mathrm{mod}\, 841) = 716$ $\theta_{16} = 24 + 627 (\mathrm{mod}\, 841) = 654$

Итак получаем зашифрованный текст: 99 92 135 195 273 395 548 716 74 320 565 28 349 688 236 654 с ключем ($a_1 = 17, a_2 = 30, s = 2, K = 7, N_1 = 256, N_2 = 841$).

Список использованных источников

1. Рублева Г.В. Математическая статистика: статистические критерии проверки гипотез. УП. Тюмень. 2014.
2. Кнут Д.Э. Искусство программирования, том 2. Получисленные алгоритмы. Пер. с англ. под общей редакцией Ю.В. Козаченко: The art of computer programming, Volume 2: Semi numerical Algorithms, 3rd Edition, Publisher: Addison-Wesley, 1998. М.: Издательский дом «Вильямс», 2001. – 832 с.
3. Фергюсон Н., Шнайер Б. Практическая криптография: Пер. с англ. М.: Издательский дом “Вильямс”, 2004.
4. Mathworld http://mathworld.wolfram.com/RandomNumber.html
5. Белова И. М. «Компьютерное моделирование» Учебно-методическое пособие для студентов направления «Прикладная математика и информатика». — М.: МГИУ, 2007.
6. Кнут Д.Э. Искусство программирования для ЭВМ, том 2. Получисленные алгоритмы. Пер. с англ. Г.П.Бабенко, Э.Г. Белаги и Л.В.Майорова, под ред. К.И.Бабенко: The art of computer programming, Volume 2: Semi numerical Algorithms, Publisher: Addison-Wesley, 1969. М.: Издательство «Мир», 1977. – 784 с.
7. Темиргалиев Н., Темиргалиева Ж. Н. Полное спектральное тестирование по методу Ковэю-Макферсона генераторов случайных чисел Лехмера с максимальным периодом. Вестник, I часть, №2(111),2016.