



ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Donetsk National Technical University
Department of higher mathematics and physics

**1st INTERNATIONAL SCIENTIFIC
AND PRACTICAL CONFERENCE**
for Students and Young Scientists

**“Mathematics and
Mathematical Simulation in a
Modern Technical University”**

Abstracts of 1st International
Scientific and Practical Conference

Lutsk, Ukraine
November 30, 2022

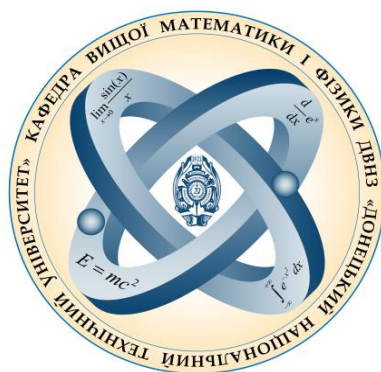
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»

ФАКУЛЬТЕТ МАШИНОБУДУВАННЯ, ЕЛЕКТРОІНЖЕНЕРІЇ ТА ХІМІЧНИХ ТЕХНОЛОГІЙ

КАФЕДРА ВИЩОЇ МАТЕМАТИКИ І ФІЗИКИ

**І Міжнародна науково-практична конференція студентів та
молодих вчених «Математика та математичне моделювання у
сучасному технічному університеті»**

30 ЛИСТОПАДА 2022 РОКУ



ЛУЦЬК, 2022

ЗМІСТ

Section 1. Mathematical modeling and research of processes in modern technologies and techniques

СИСТЕМА ТЕСТ-МЕНЕДЖМЕНТУ ЯК ІНСТРУМЕНТ ДЛЯ КЕРУВАННЯ ТЕСТУВАННЯМ <i>В.О. Читулян, О.А. Золотухіна</i>	11
РОЗРОБКА ПРОГРАМИ ДЛЯ МЕНЕДЖМЕНТУ СЕРВІСНОГО ЦЕНТРУ <i>О.О. Сергієнко, Л.Г. Сергієнко</i>	13
MATHEMATICAL MODELLING OF FORM CHANGE PROCESSES IN PALADIUM PLATE <i>О.М. Lyubimenko, E.P. Feldman</i>	16
STRONG TOPOLOGICAL EQUIVALENCE OF RANDOM DYNAMICAL SYSTEMS <i>I. Vasylieva</i>	18
БІОІНФОРМАТИКА – НАУКА ЧИ МЕТОД <i>Н.О. Кузьмич, Ю.В. Новікова</i>	20
КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ РОБОТИ ВІТРОГЕНЕРАТОРА <i>О.М. Любименко, О.А. Штена</i>	22
МОДЕЛЮВАННЯ ПРОЦЕСІВ МОНІТОРИНГУ ДАНИХ З НЕЗАЛЕЖНИМ АГРЕГАТОРОМ <i>М.В. Оболонський, О.А. Дмитрієва</i>	24
РІШЕННЯ ПРОБЛЕМИ ОПРАЦЮВАННЯ ДОВГИХ ЧИСЕЛ В АСИМЕТРИЧНИХ КРИПТОСИСТЕМАХ <i>Є.В. Павловський</i>	26
РОЗВИТОК СВІТОВОГО РИНКУ ІТ-ТЕХНОЛОГІЙ <i>С.О. Савукова, Н.Ф. Гоголева</i>	28
ПОБУДОВА АНАЛІТИЧНИХ МОДЕЛЕЙ АЛГОРИТМІВ ТА ОЦІНКА ЇХ СКЛАДОВИХ <i>О.О. Сергієнко, І.А. Назарова, Л.Г. Сергієнко</i>	30
ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ WEB-СЕРВЕРУ <i>Д.А. Стреляєв, В.І. Костін</i>	33
АСИМЕТРИЧНИЙ МЕТОД ШИФРУВАННЯ. АЛГОРИТМ RSA, ВИКОРИСТАННЯ ПАКЕТУ WOLFRAM MATHEMATICA ДЛЯ ГЕНЕРУВАННЯ ВЕЛИКИХ ПРОСТИХ ЧИСЕЛ В КРИПТОГРАФІЇ <i>Є.Р. Терехов, Т.В. Скрипник</i>	37
ЗАСОБИ ТОПОЛОГІЧНОГО АНАЛІЗУ МІМД-СИМУЛЯТОРА МЕРЕЖЕВОГО ДИНАМІЧНОГО ОБ'ЄКТУ З ЗОСЕРЕДЖЕНИМИ ПАРАМЕТРАМИ (МДОЗП) <i>Ю.Г. Тихонова</i>	40

МАТЕМАТИЧНИЙ ПАРАДОКС МОНТІ ХОЛЛА В PYTHON <i>М.В. Тютюнник, Ю.В. Новікова</i>	43
ПРО ДОВЖИНУ СПІРАЛІ АРХІМЕДА ТА ПАРАБОЛИ <i>О.О. Циплаков, С.В. Волков</i>	45
МОДЕЛЮВАННЯ ТА РОЗРОБКА СИСТЕМИ АНАЛІЗУ ЗВОРОТНОГО ЗВ'ЯЗКУ КОРИСТУВАЧІВ МЕРЕЖІ ІНТЕРНЕТ <i>І.В. Ярош, Т.О. Черняк</i>	47
РОЗРОБКА НЕЧІТКОЇ МОДЕЛІ ПРОГНОЗУВАННЯ КІЛЬКОСТІ РОБІТ В ПРОЦЕСІ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ КОМП'ЮТЕРНОЇ ТЕХНІКИ НА ПІДПРИЄМСТВІ <i>І.В. Ярош, Т.О. Черняк</i>	49
ДОСЛІДЖЕННЯ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ЗАХИСТУ WEB-ДОДАТКІВ НА ОСНОВІ JS <i>О. Ясинський, Н. О. Маслова</i>	52
 Section 2. Mathematical modeling and research of economic processes in the context of modern problems and requirements of society	
ЛОГІСТИЧНА МОДЕЛЬ ЗАКОНУ РОЗМНОЖЕННЯ ПОПУЛЯЦІЇ <i>А.О. Деркунська, Є.В. Лесіна</i>	56
МЕТОДИ МАКСИМІЗАЦІЇ ПРИБУТКУ НА ПІДПРИЄМСТВІ В УМОВАХ ОБМЕЖЕНОСТІ РЕСУРСІВ <i>К.К. Кузнецова, Л.Д. Сарбаш</i>	58
ECONOMIC AND STATISTICAL ANALYSIS OF THE UNEMPLOYMENT RATE IN SOME COUNTRIES OF THE EUROPEAN UNION <i>Sofiiia Burian, Nataliia Hoholieva</i>	60
ESTIMATION OF ALL PARAMETERS IN THE VASICEK MODEL BY LOW-FREQUENCY DATA <i>O.D. Prykhodko, K.V. Ralchenko</i>	62
МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ В ЕКОНОМІЦІ ТА УПРАВЛІННІ ЯК ЗАСІБ ФОРМУВАННЯ ФАХОВОЇ КОМПЕТЕНЦІЇ ЗДОБУВАЧІВ ЕКОНОМІЧНИХ СПЕЦІАЛЬНОСТЕЙ <i>А.О. Бондаренко, А.В. Тарасенко, О.Г. Ровенська</i>	64
ОПТИМІЗАЦІЯ ВИКОРИСТАННЯ РЕСУРСІВ НА ПІДПРИЄМСТВАХ ЗА ДОПОМОГОЮ ДИНАМІЧНОГО ПРОГРАМУВАННЯ <i>Т.В. Ворона, Л.Д. Сарбаш</i>	68
МАТЕМАТИЧНІ ОСНОВИ НА СТРАХОВОМУ РИНКУ <i>М.О. Єнін, Ю.В. Новікова</i>	70

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ДИНАМІКИ РОЗВИТКУ ЕПІДЕМІЇ <i>Є.А. Мерзлікіна, Є.В. Лесіна</i>	73
SPAIN QUALITY OF LIFE INDEX ANALYSIS <i>V.M. Ponchko, N.F. Hoholieva</i>	76
SPAIN ECONOMIC DEVELOPMENT: REGRESSION ANALYSIS OF GDP <i>A.O. Chub, N.F. Hoholieva</i>	78
ЕКОНОМІКО-МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ В ДОСЛІДЖЕННІ ІНФЛЯЦІЙНИХ ПРОЦЕСІВ <i>В.О. Христюк, І.Г. Сивицька</i>	80
ЗАСТОСУВАННЯ МЕТОДУ НАЙМЕНШИХ КВАДРАТІВ ПРИ ДОСЛІДЖЕННІ ЛІНІЙНОЇ БАГАТОФАКТОРНОЇ МОДЕЛІ <i>Т. Г. Поначевна, Є.В. Лесіна</i>	82
Section 3. Technologies and methods of teaching mathematics at a modern Technical University, features of teaching in distance learning	
ВИКОРИСТАННЯ ІНТЕРАКТИВНИХ ОНЛАЙН-ДОШОК ПРИ ВИКЛАДАННІ МАТЕМАТИЧНИХ ДИСЦИПЛІН В ОСВІТНЬОМУ ПРОЦЕСІ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ <i>Ю.С. Дерябіна, Н.В. Кравченко</i>	85
ВИКОРИСТАННЯ ПРОГРАМИ «STUDENT» У ПРОЦЕСІ ВИКЛАДАННЯ ФІЗИКИ <i>Ю.М. Лимарєва, В.В. Недоступ, О.Я. Белошапка</i>	88
ОСОБЛИВОСТІ ВИКОРИСТАННЯ ГРАФА ЗНАНЬ У НАВЧАННІ <i>Є.В. Ролдугін, О.А. Золотухіна</i>	90
ОСОБЛИВОСТІ ДЕМОНСТРАЦІЙНОГО ЕКСПЕРИМЕНТУ НА УРОКАХ ФІЗИКИ <i>Ю.М. Лимарєва, Д.Н. Саакян, О.Я. Белошапка</i>	92
МОДЕЛЮВАННЯ ГАРМОНІЧНИХ КОЛИВАНЬ ФІЗИЧНОГО МАЯТНИКА ЗА ДОПОМОГОЮ ПРОГРАМИ SOLIDWORKS <i>О.В. Сергієнко, М.М. Власенко</i>	94
КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ І ДОСЛІДЖЕННЯ ЗГАСАЮЧИХ КОЛИВАНЬ ПРУЖИННОГО МАЯТНИКА <i>М.І. Сінявський, М.М. Власенко</i>	97
СТВОРЕННЯ КОМП'ЮТЕРНОЇ МОДЕЛІ МАШИНИ АТВУДА І ДОСЛІДЖЕННЯ КІНЕМАТИКИ І ДИНАМІКИ ПОСТУПАЛЬНОГО РУХУ <i>С.Є. Федоренко, М.М. Власенко</i>	100

АСИМЕТРИЧНИЙ МЕТОД ШИФРУВАННЯ. АЛГОРИТМ RSA, ВИКОРИСТАННЯ ПАКЕТУ WOLFRAM MATHEMATICA ДЛЯ ГЕНЕРУВАННЯ ВЕЛИКИХ ПРОСТИХ ЧИСЕЛ В КРИПТОГРАФІЇ

Є.Р. Терехов, студент ОП «Кібербезпека»

Т.В. Скрипник, старший викладач кафедри ПМІ

Донецький національний технічний університет, Луцьк, Україна

Анотація. Досліджується найпоширеніший алгоритм асиметричного шифрування RSA. Стійкість RSA базується на складності факторизації великих цілих чисел. RSA можна застосовувати як для шифрування/розшифрування, так і для генерації/перевірки електронного цифрового підпису (ЕЦП).

Ключові слова: шифрування, алгоритм RSA, відкритий ключ, просте число, дешифрування.

Вступ. На сьогодні асиметричне шифрування на основі відкритого ключа RSA (розшифровується, як Rivest, Shamir and Aldeman – творці алгоритму) використовує більшість продуктів на ринку інформаційної безпеки.

Його криптостійкість ґрунтується на складності розкладання на множники великих чисел, а саме - на винятковій важкості завдання визначити секретний ключ на основі відкритого, тому що для цього потрібно розв'язати задачу існування дільників цілого числа. Найбільш криптостійкі системи використовують 1024-бітові та великі числа.

Мета. Дослідити роботу алгоритму RSA за критерієм швидкодії, зокрема генерування простих чисел для формування ключів шифрування, засобами пакету Wolfram Mathematica.

Основна частина. З практичної точки зору алгоритм RSA можна поділити на два етапи, кожен з яких складається з кількох кроків. Це етапи генерування відкритого та секретного ключів і, власне, шифрування повідомлення.

Етап генерування ключів покроково виглядає так:

- Візьмемо два великі прості числа p та q порядку 2^{768} та 2^{1024} відповідно до кожного (рис. 2).
- Розрахуємо n , як результат добутку p і q ($n = p*q$) (рис. 3).
- Виберемо випадкове число, яке назовемо d . Це число має бути взаємно простим (тобто, не мати жодного спільного дільника, крім 1) із результатом добутку $(p-1)*(q-1)$.
- Визначимо таке число e , для якого є істинним наступне співвідношення $(e*d) \bmod ((p-1)*(q-1)) = 1$.
- Назвемо відкритим ключем числа e і n , а секретним - d і n .

Для процесу шифрування повідомлення за відкритим ключем $\{e, n\}$ слід виконати наступні дії:

- розбити текст, що шифрується, на блоки, кожен з яких може бути представлений у вигляді числа $M(i) = 0, 1, 2, \dots, n-1$ (рис. 1).
- зашифрувати текст, що розглядається як послідовність чисел $M(i)$ за формулою $C(i) = (M(i)^e) \bmod n$ (рис. 4).

Для того, щоб розшифрувати отриману криптограму, використовуючи секретний ключ $\{d, n\}$, необхідно виконати такі обчислення $M(i) = (C(i)^d) \bmod n$. В результаті чого буде отримано множину чисел $M(i)$, що відповідатиме при певній конвертації вхідному тексту. В якості вхідного повідомлення біло обрано ПБ автора «Терехов Єгор Русланович».

Опис пропозиції. Алгоритми шифрування з відкритим ключем у середньому працюють у тисячі разів повільніше за симетричні алгоритми, а також вони вимогливі до пам'яті та обчислювальної потужності комп'ютера. Ця особливість була досліджена спробами рандомізації простих чисел особливо великих порядків для формування пари ключів засобами програмування на мовах C++ та Python. Оскільки програми працювали надзвичайно довго і не завжди видавали очікуваний результат, то було обрано рішення скористуватися потужними засобами програми «Wolfram Mathematica», що може опрацьовувати доволі великі числа.

Застосовуючи функціональні можливості означеної програми було представлено описаний метод шифрування.

Рядок повідомлення та множина числових блоків $M(i)$, відповідно до кожного символу вхідного тексту подано на рис. 1.

```
In[1]:= str = "Терехов Єгор Русланович"
      M = ToCharacterCode[str]

Out[1]= Терехов Єгор Русланович

Out[2]= {1058, 1077, 1088, 1077, 1093, 1086,
      1074, 32, 1028, 1075, 1086, 1088, 32, 1056, 1091,
      1089, 1083, 1072, 1085, 1086, 1074, 1080, 1095}
```

Рис. 1. Рядок відкритого тексту та кодування символів у числові блоки

Генерування простих чисел означених вище порядків наведено на рис. 2.

```
In[3]:= p = NextPrime[2^768]

Out[3]= 1552518092300708935148979488462502555256886017116696611 :
      139052038026050952686376886330878408828646477950487730 :
      697131073206171580044114814391444287275041181139204454 :
      976020849905550265285631598444825262999193716468750892 :
      846853816058039

In[4]:= q = NextPrime[2^1024]

Out[4]= 179769313486231590772930519078902473361797697894230657273 :
      430081157732675805500963132708477322407536021120113879 :
      871393357658789768814416622492847430639474124377767893 :
      424865485276302219601246094119453082952085005768838150 :
      682342462881473913110540827237163350510684586298239947 :
      245938479716304835356329624224137859
```

Рис. 2. Генерування простих чисел p і q

Формування параметрів системи RSA подано на рис. 3.

```
In[5]:= n = p * q
Out[5]:= 279095111627852376407822673918065072905887935345660252615 \
989519488029661278604994789701101367875859521849524793 \
382568057369148405837577299984720398976429790087982805 \
274893437406788716103454867635208144157749912668657006 \
085226160294706625852843084369218264705363016445247708 \
352165200176022381626250444607084964470181341019003003 \
415598483967897657554394321071280340452051898833108957 \
724846122456100123936170740252983449524382165752876265 \
876496572523442181968085530164687457504983765791136126 \
377958572067585002096597551704523428264564681198501

In[6]:= phi = (p - 1) (q - 1)
Out[6]:= 279095111627852376407822673918065072905887935345660252615 \
989519488029661278604994789701101367875859521849524793 \
382568057369148405837577299984720398976429790087982805 \
274893437406788716103454867635208144157749912668657006 \
085226160294526856539356852778445334186284113971885910 \
654270969518748951545092711931279461954530540240971660 \
730597875391515230904150645164814914896377367959627365 \
564344858357328290242038986000276117581156973093621733 \
747375989293847212350581467551569891988135678722235350 \
407740675382812493158924118930937179088086641002604
```

Рис. 3. Модуль перетворення n , як добуток p і q та функція $\phi(n)$

Обчислення криптограми відбувається в циклі, що подано на рис. 4.

```
In[12]:= CC = Table[0, {i, 1, Length[M]}];
For[i = 1, i <= Length[M], i++,
{CC[[i]] = PowerMod[M[[i]], e, n]}];
];
CC // MatrixForm
Out[14]//MatrixForm=
83 431 762 204 965 288 967 315 426 483 304 720 780 304 986 589 491 404 228 745 \
276 720 968 585 444 070 141 262 568 582 971 937 931 566 952 407 487 809 793 216 \
132 525 465 987 745 554 388 301 175 172 966 048 827 559 230 268 739 584 624 433 \
276 720 968 585 444 070 141 262 568 582 971 937 931 566 952 407 487 809 793 216 \
250 395 406 270 577 612 099 110 976 133 527 752 251 201 352 273 862 485 411 141 \
80 631 913 396 459 607 355 418 876 403 171 826 429 056 221 429 401 546 748 842 \
51 593 439 381 850 208 248 700 726 957 498 080 587 983 465 854 087 461 074 227 \
48 259 808 447 793 508 648 390 773 931 006 769 445 198 973 927 364 893 530 825 \
96 909 212 277 938 900 439 324 642 844 766 325 460 893 162 885 313 195 935 426 \
46 847 043 327 944 693 454 619 248 505 360 648 995 289 496 128 349 958 130 471 \
80 631 913 396 459 607 355 418 876 403 171 826 429 056 221 429 401 546 748 842 \
132 525 465 987 745 554 388 301 175 172 966 048 827 559 230 268 739 584 624 433 \
48 259 808 447 793 508 648 390 773 931 006 769 445 198 973 927 364 893 530 825 \
181 824 940 532 759 845 755 501 119 888 251 612 761 978 718 052 485 463 868 432 \
54 914 805 321 993 900 852 437 207 348 882 557 362 491 602 883 543 327 559 223 \
191 914 503 291 132 628 498 449 704 911 311 146 974 775 606 171 840 300 697 287 \
17 045 175 972 840 018 465 126 581 317 897 128 698 873 128 499 286 734 800 577 \
38 604 271 480 693 892 136 530 715 684 041 156 327 404 512 996 770 708 988 240 \
99 716 394 469 723 439 717 911 554 942 024 576 350 521 279 381 391 721 412 447 \
80 631 913 396 459 607 355 418 876 403 171 826 429 056 221 429 401 546 748 842 \
51 593 439 381 850 208 248 700 726 957 498 080 587 983 465 854 087 461 074 227 \
150 476 505 433 508 250 100 173 952 480 711 865 417 637 843 430 987 787 109 846 \
232 316 967 410 062 146 442 996 977 199 005 218 981 712 768 326 335 650 085 404
```

Рис. 4. Формування криптограми

Висновки. Серед найбільш відомих недоліків алгоритму RSA можна виділити некоректний вибір значень p і q . Числа p і q мають бути простими і не міститися в жодній з відомих таблиць простих чисел. Ці числа також не повинні бути близькими один до одного, бо це впливає на стійкість алгоритму шифрування.

Перелік посилань

1. Тарнавський Ю.А. Технології захисту інформації / Київ, КПІ ім. Ігоря Сікорського – 2018 – 161 с.
2. Барич, С. Г. Основи сучасної криптографії: навчань, курс / С. Г. Барич, В. В. Гончаров, Р. Є. Серов. - М: Горяча лінія - Телеком, 2011.
3. Рябко, Б. Я. Криптографічні методи захисту інформації / Б. Я. Рябко.

Наукове видання

**«Математика та математичне моделювання у сучасному
технічному університеті»**

Збірник тез доповідей

**I Міжнародної науково-практичної конференції студентів та молодих
вчених**

30 листопада 2022 року, м. Луцьк

Технічна обробка, комп'ютерний набір, верстка: Гогольова Наталія Федорівна

Оригінал-макет виготовлено на кафедрі вищої математики і фізики
ДВНЗ «Донецький національний технічний університет»

Формат А4