УДК: 61 : 651. 928: 681. 3I: 003.26 : 681. 3I: 007

МАТЕМАТИЧНІ АЛГОРИТМИ ЗАХИСТУ ІНФОРМАЦІЇ

І. М. Шупяцький

Державна служба спеціального зв'язку та захисту інформації України

У статті проаналізовано математичні алгоритми захисту інформації з метою використання методології алгоритму криптографії в медицині.

Ключові слова: криптографія, алгоритм, ключ, методологія.

МАТЕМАТИЧЕСКИЕ АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ

И. М. Шупяцкий

Государственная служба специальной связи и защиты информации Украины

В статье проанализированы математические алгоритмы защиты информации с целью использования методологии алгоритма криптографии в медицине.

Ключевые слова: криптография, алгоритм, ключ, методология.

MATHEMATICS ALGORITHMS OF THE INFORMATION PROTECTION

I. M. Shupiatskyi

State department of the special connect & protection information of Ukraine

There were discussed mathematics algorithms of the information protection with purpose to use the main methods of the cryptography algorithm in the medicine.

Key words: cryptography, algorithm, key, main methods.

Присвячується 120-річчю засновника сучасних математичних методів криптографії, академіку АН УРСР М. П. Кравчуку.

Вступ. На сьогодні захист інформації здійснюється за допомогою та на основі сучасних техніко-економічних криптографічних засобів. Медична інформація - це інформація конфіденційна, яка потребує цілеспрямованого захисту, захисту криптографічного в сучасному інформаційному просторі. Мета захисту - недопущення використання медичної інформації особами, які не мають права доступу до конфіденційних ресурсів.

Одним із основних методів сучасних криптографічних алгоритмів є прикладна теорія чисел, яка є фундаментом сучасних математичних криптографічних алгоритмів. При обміні інформацією між учасниками часто виникає ситуація, коли інформація не є конфіденційною, а саме, - отримання повідомлень у неперекрученому вигляді і наявність гарантії, що ніхто не в змозі підробити повідомлення.

Мета роботи полягає в проведенні аналізу математичних алгоритмів захисту інформації для можливостей використання методології алгоритму криптографії в медицині.

Отримані результати та їх обговорення. Криптосистеми із секретним ключем (одноключові, симетричні або класичні), а також криптосистеми з відкритим ключем (асиметричні) максимально адаптовані до використання з метою захисту і збереження інформації. Як приклад можна навести основні положення криптологічного протоколу "електронний підпис".

Математична криптографія виникла як наука про шифрування інформації, - як наука про криптосистеми.

Криптосистема без передачі ключів.

Абоненти A, B, C, ... домовились організувати закрите листування між собою. Для цього вони вибрали достатньо велике просте число p і таке, що p-1 добре розкладається на не дуже великі прості множники. Якщо серед множників такого числа кратних немає, то число p-1 називають Евклідовим. Кожний з абонентів, незалежно один від одного, вибирає випадкове число, натуральне, взаємно просте з числом p-1: A, B, C, ... - абоненти; a, Ь, c, ... - вибрані ними

випадкові числа. В подальшому абонент А знаходить число α з умов

$$a\cdot\alpha\equiv 1(\mathrm{mod}\ \phi(p)),\ 0<\alpha<p-1; \qquad (1)$$

абонент В знаходить число в з умови

$$b\cdot\beta\equiv 1(\mathrm{mod}\ \phi(p)),\ 0<\beta<p-1, \qquad (2)$$

де ф(р) - функція Ейлера, а, α - закриті ключі абонента А; b, β - закриті ключі абонента В тощо.

У тому випадку, коли абонент А вирішує надіслати повідомлення т абоненту В можна прогнозувати, що 0 < m < р-1. Тоді він спочатку зашифровує це повідомлення своїм першим закритим ключем, знаходить:

$$m_1\equiv m^a(\mathrm{mod}\ p),\ 0<m_1<p \qquad (3)$$

і направляє абоненту В. Абонент В, в свою чергу, зашифровує знову це повідомлення також своїм першим ключем:

$$m_2\equiv m_1^{б}(\mathrm{mod}\ p),\ 0<m_2<p \qquad (4)$$

і пересилає його у зворотному напрямку абоненту А. Абонент А, отримавши своє подвійно зашифроване повідомлення, шифрує його ж втретє своїм другим ключем:

$$m_3\equiv m_2^{\alpha}(\mathrm{mod}\ p),\ 0<m_3<p \qquad (5)$$

і знову відправляє його абоненту В. Останній розшифровує цю шифротелеграму за допомогою свого другого ключа:

$m_4\equiv m_3^{\beta}(\mathrm{mod}\ p),\ 0<m_4<p$.

Таким чином, з порівняння (3) - (4) маємо:

$m_4\equiv m^k(\mathrm{mod}\ p)$,

де $k\equiv a\cdot\alpha\cdot b\cdot\beta(\mathrm{mod}\ p-1)$.

В силу (1) і (2) $k\equiv 1(\mathrm{mod}\ \phi(p))$. Тому $n_4\equiv m(\mathrm{mod}\ p)$ а так як кожне з них позитивне і менше р, то $т_4=т$.

Наприклад, нехай абоненти А і В вирішили встановити між собою прихований зв'язок без передачі ключів. Вони вибрали для цього просте число р = 9551. Тоді р-1=9550.

Абонент А вибирає випадкове число α=8159, а абонент В - b=7159. Абонент А вирішує рівняння: $8159\cdot\alpha\equiv 1(\mathrm{mod}\ \phi(9551))$, $0<\alpha<9550$ й знаходить α= 6639, а абонент В вирішує рівняння: 7159 $\beta\equiv 1(\mathrm{mod}\ \phi(9551))$, $0<\beta<9550$ й знаходить β= 6139.

Абонент А вирішує надіслати секретне повідомлення абоненту В т=7032. Тоді він спочатку шифрує повідомлення своїм першим ключем: $m_1\equiv m^a(\mathrm{mod}\ p)$= 7032^{81593}(mod 9551)= 153.

Абонент В, отримавши це повідомлення, шифрує його своїм першим ключем: $m_2\equiv m_1^{b}(\mathrm{mod}\ p)$= 153^{7159}(mod 9551)= 4896, і пересилає його абоненту А, який, отримавши зашифроване повідомлення, шифрує його ж в третій раз своїм другим ключем: $т_3\circ т_2^{a}$(тоа р) =4896^{6639}(тоа 9551)= 7577 і відправляє його абоненту В, який розшифровує цю шифротелеграму за допомогою свого другого ключа: $т_4\circ т$/(тоа р)= 7577^{6139}(тоа 9551)= 7032.

Розглянемо схожий приклад, але з великими числами, а саме нехай абоненти А і В вибирають випадкове число р =3 61850278866613110698659328152149712041468702080126762623304950024728530131З. Далі абонент А вибирає випадкове число а=32910091146 42412084309938365114701009965471731267159726697218119, а абонент В- Ь=7 21334567291943120091146424456567812084309346479383651654546 5843. АбонентА вирішує рівняння: 3291009114642412084309938365114701009965 4717312671 59726697218119-а°1(тоа ф(361850278 86661311069865932815214971204146870208012676262330495002472853013 13)), 0 < а < 3618502 788 66613110698659328152149712041468702080126762623304950024728530131 2 і знаходить а=7182890 94672427671226754071206041429575840582 862 25696133 69504272231654775, а абонент В вирішує рівняння: 721334567291943120091146 42445656781 208430934647938365165454 65843-р °1(тоа ф(119726 214130147567059245861496117904970213993920 59391)), 0 < р <119726214130 1475670592458614961179 049702139939205 9390 і знаходить р= 205078500 89479826167721544736489099017840580106896795952493654865076402209 87.

Абонент А вирішує надіслати секретне повідомлення абоненту В т=16439530856237023359734047455621923453212389086. Тоді він с початку шифрує повідомлення своїм першим ключем: $т_1\circ m^a$(mod р)= 164395308 56237023359734047455621 92345321 2 3 8 9 0 8 6 32910091146424120843099383651147010099654717312671597266972181 19(mod 36185027886661311069865 932815214971204146870208012676262330495 0 0247285 301313)= 234048847172608960712455675626416933820229094970133 561697306266457241 4115995.

Абонент В, отримавши це повідомлення, шифрує його своїм першим ключем: $m_2\circ m_1^{a}$(mod р)= 234048847172608960712455675626416933820229 0949 $^{70133561697306266457241411599572133456729194312009114642445656781208430934647938365165454 65843}$(mod 36185027886661311069865 932815214971204146870208012676262330495002472853013 13) =200847152309106133691890020899 385 1807662985672512619192514870979350742436070, і пересилає його абоненту А. Абонент А, отримавши зашифроване повідомлення, шифрує його ж в третій раз своїм другим ключем: $m_3\circ m_2^{a}$(mod р)

=2008471523091061336918900208993851 8076629 8567251261919251487097935074243607071828909467242767122675407120604142099575840582862256961336950427231654775(mod 3618502788666131106986593281521497120414687020801267626233049500247285301313)=3374267 95 6 0 6 6 4 0 4 4 9 1 4 4 3 9 6 3 9 2 1 3 5 6 2 0 3 6 4 9 7523303647522251966113925361609484371961643953085623702335973404745562192345321238908616439530856237023359734047455621923453212389086

Прикладом можуть служити паперові купюри. Як що ресурсом є деякий товар, то наявність у покупця достатньої кількості купюр є доказом його права на доступ до ресурсу. З іншої сторони, хоча кожна паперова купюра і має унікальний номер, відслідкувати купюри за номерами та виявити, хто її використав і в яких платежах, практично неможливо.

Висновки. 1. Для запобігання загрозі контролю за джерелами інформації (звідки пересилаються повідомлення) необхідна система контролю за доступом до ресурсів, яка повинна задовольняти двом, здавалося б, взаємно протилежним потребам.

2. Кожен бажаючий повинен мати можливість звернутися до цієї системи анонімно, при цьому все ж довівши своє право на доступ до ресурсів.

3. Якщо задача забезпечення конфіденційності вирішується за допомогою криптосистем, то для забезпечення цілістності і унеможливлення відслідковування розробляють криптографічні протоколи. Адаптація криптографічних алгоритмів до телемедицини дасть можливість впровадження нових наукових та практичних досягнень, продуктом яких слід очікувати телемедичний алгоритм в криптографії, де основою є поліном М. П. Кравчука.

Література.

1. Анализ современных зарубежных систем защиты информации / под ред. *В. Ф. Колчина.* // Обозрение прикл. и промышл. матем. - 2000. - Т. 7.

2. Вероятностно-статистический анализ последовательностей над конечным алфавитом / под ред. *В. Г. Михайлова, В. П. Чистякова.* // Обозрение прикл. и промышл. матем. - 1995. - Т. 2.

3. Конечные автоматы: прообразы выходных последовательностей над конечным алфавитом / под ред. *В. Г. Михайлова, В. П. Чистякова.* // Обозрение прикл. и промышл. матем. - 1995. - Т. 1.

4. Методы дискретной теории вероятностей / под ред. *А. М. Зубкова.* // Обозрение прикл. и промышл. матем., 1996, т. 3. в. 4.

5. Новые подходы к решению вероятностных задач. Под ред. *А. М. Зубкова.* // Обозрение прикл. и промышл. матем.. - 1994. - Т. 1, В. 4.

6. Пороговая логика и нейрокомпьютеры. / под ред. *Г. В. Балакина.* // Обозрение прикл. и промышл. матем. - 1994. - Т.1, В. 3.

7. Браун П. Приватность в век терабайтов и терроризма / Питер Браун // В мире науки. - 2008. - №> 12. - С. 20-21.

8. Ванчаков Н. Б. Практические основы защиты информации. Технические методы и средства : производственно - практическое издание / Н. Б. Ванчаков, А. Н. Григорьев.- Калининград : КЮИ МВД России, 2000. - 198 с.

9. Голубев Д. Л. Распределенные центры обработки данных / Голубев Д. Л. // Jet Info. - 2006. - №> 5. - С. 3-16.

10. Горбатов В. С. Основы технологии PKI / В. С. Горбатов, О.Ю. Полянская. - М. : Горячая линия - Телеком, 2004 - 246 с.