УДК 623.618:355.311.6

І. Ю. РОЗУМ, *кандидат військових наук, начальник науково-дослідної лабораторії проблем розвитку систем зв'язку та автоматизованих систем управління інституту інформаційних технологій Національного університету оборони України імені Івана Черняховського, м. Київ*

ЗАСТОСУВАННЯ ПРИКЛАДНОЇ КРИПТОГРАФІЇ В СИСТЕМІ ВІЙСЬКОВОГО УПРАВЛІННЯ В ІНТЕРЕСАХ ЗАСЕКРЕЧУВАННЯ МЕРЕЖ ЗВ'ЯЗКУ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

У статті розглянута можливість застосування прикладної криптографії щодо впровадження асиметричних алгоритмів шифрування та криптографії з відкритим ключем у системі військового управління з метою засекречування мереж зв'язку військового призначення.

Ключові слова: *система військового управління, криптографія, засекречування мереж військового зв'язку, теорія порівнянь, алгоритми шифрування.*

Постановка проблеми у загальному вигляді. Реалії сьогодення не виключають можливості виникнення збройних протистоянь як засобу розв'язання міждержавних, релігійних, етнічних та інших протиріч. Успіх у сучасній війні залежить не тільки від співвідношення сил, майстерності фахівців військового управління, інновацій засобів ураження і оснащення ними військ, а й від засекречування інформації в системі військового управління [1].

Як відомо, інформація ще з давніх часів була суттєвою цінністю. Сучасні технології дають можливості її передавати і зберегти у значних об-

сягах. Між цим вона стає все більш уразливою, що також має і зворотний бік, а причини криються у такому: зростають обсяги інформації (даних), які зберігаються та передаються; розширюється коло користувачів, які мають доступ до інформації; ускладнюється режим експлуатації обчислювальної техніки. З цього приводу і виникає необхідність засекречування інформації під час її передачі та збереження.

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми та на які опирається автор. Взагалі під поняттям "засекречування інформації" розуміється сукупність застосування заходів, методів і засобів захисту, що забезпечують безпеку інформації, перевірку її цілісності та виключення можливого несанкціонованого доступу до програм, які використовуються. Один із раціональних методів засекречування інформації – шифрування (криптографія), який полягає у перетворенні відкритих даних у шифровані і навпаки, що прийнято називати шифруванням, де дві складові цього процесу прийнято називати, відповідно, шифруванням та розшифруванням. Акцентуємо, що криптографічна система є невід'ємною частиною безпеки військового управління та, як правило, складається зі взаємооднотипного перетворення $k_{з.д}$, яке шифрується з безлічі P всіх можливих елементів відкритого тексту з множиною C усіх можливих елементів шифрованого тексту [2].

Насамперед, термін "криптосистема" частіше застосовується до цілого сімейства таких перетворень, залежних від вибору деяких параметрів (від них можуть залежати як відображення $T_{пз}$, так і безлічі P і C). Наприклад, при фіксованому N – буквеному алфавіті можна розглядати афінна криптосистему, яка при кожному $a \in \left(Z_{/NZ}\right)^*$ і $b \in Z_{/NZ}$ є відображенням з $P = Z_{/NZ}$ в $C = Z_{/NZ}$, заданим виразом $C \equiv aP + b(\mathrm{mod}\, N)$. У даному прикладі множини P і C фіксовані (оскільки N фіксоване число), але перетворення f, яке шифрується, залежить від вибору параметрів a і b. Тому перетворення, яке шифрується, можна задавати алгоритмом, єдиним для всього сімейства, і значенням параметрів. Значення параметрів називається ключем шифрування K_E. У нашому прикладі – K_E пара (a, b).

Для дешифрування, тобто обчислення f^{-1}, також необхідні алгоритм і ключ. Даний ключ називається ключем дешифрування K_D. У нашому прикладі афінна криптосистема дешифрування проводить афінне перетворення $P \equiv a^{-1}C - a^{-1}b(\mathrm{mod}\, N)$, тобто алгоритм дешифрування співпадає

з алгоритмом шифрування, але з іншим ключем, а саме $(a^{-1}, -a^{-1}b)$. У деяких криптосистемах алгоритм дешифрування, як і ключ, відрізняється від алгоритму шифрування. Ми припускатимемо, що алгоритми шифрування і дешифрування загальновідомі, а приховані лише ключі K_E і K_D [3].

Припустимо, що хтось намагається використовувати для засекречування описану вище афінну криптосистему $C \equiv aP + b$. Як показано в [4] дану систему неважко розкрити, якщо використовувати однолітерні елементи тексту в N – буквеному алфавіті. Набагато складніше розкрити дану систему при використанні біграм, що можна розглядати як використання N^2 – буквеного алфавіту. Краще використовувати блоки з k букв з числовими еквівалентами з $Z_{N^k Z}$. При $k > 3$ використовувати частотний аналіз вже скрутніше, оскільки число можливих до k-грам безліч, і багато з них можна з рівною підставою вважати такими, що найбільш часто зустрічаються. Якщо йти по шляху збільшення k, то необхідно враховувати витрати часу на розв'язання різних арифметичних задач (найважливіша з них – отримання a^{-1} за допомогою алгоритму Евкліда) як при виборі ключів, так і при шифруванні та дешифруванні кожного повідомлення.

В усіх криптосистемах, що використовувались більш чверть століття, не було потреби задавати ключ дешифрування, якщо ключ і алгоритм шифрування були відомі. Навіть маючи справу з такими великими числами, як N^k, при дуже великому k, можна визначити ключ дешифрування за ключем шифрування за час, який близький за порядком до часу роботи стандартних алгоритмів. Наприклад, у випадку афінного перетворення в $Z_{N^k Z}$, знаючи ключ шифрування $K_E = (a, b)$, можна обчислити ключ дешифрування $K_D = (a^{-1} (\mathrm{mod}\, N^k) - a^{-1} b (\mathrm{mod}\, N^k))$ за допомогою алгоритму Евкліда $O(\log^3 N^k)$ двоїчних операцій. Таким чином, у традиційних криптосистемах можливості дешифрувати повідомлення можна з невеликими зусиллями або зовсім без них визначити ключ шифрування. Проте в 1976 році Деффі і Хелман відкрили принципово новий тип криптосистем і розробили "криптографію з відкритим ключем" [4].

За визначенням, криптосистема з відкритим ключем володіє тією властивістю, що знання шифруючого перетворення не дозволяє за ключем шифрування знайти ключ дешифрування, уникнувши надзвичайно довгих обчислень. Іншими словами, шифруюча функція $f : P \to C$ легко обчислюється, якщо ключ шифрування K_E відомий, але обчислювати значення

зворотної функції $f^{-1}: C \to P$ дуже складно. З погляду практичного обчислення це означає, що функція f незворотна. Таким чином, функція f – це легкообчислювальна функція, для якої зворотну функцію f^{-1} обчислити важко, якщо не мати деякої додаткової інформації, що використовується при обчисленні f. Зворотна функція f^{-1} легко обчислюється, якщо відома додаткова інформація K_D – ключ дешифрування. Дуже близьким є поняття однонапрямкова функція. Це така функція, яку легко обчислити, але для якої зворотну функцію f^{-1} обчислити важко навіть за наявності деякої додаткової інформації. У 1978 році розроблена криптосистема *RSA* з відкритим ключем [5]. У 1974 році Дж. Парді вперше детально описав таку однонапрямкову функцію. Початковий пароль і зашифрований пароль розглядаються як цілі числа за великим простим модулем *p*, а однонаправлені відображення $F_p \to F_p$ задаються багаточленом *f(x)*, який неважко обчислити на комп'ютері, але обернути його за розумний час неможливо. Дж. Парді використовував $p = 2^{64}\text{-}59$, де коефіцієнтами є довільні 19-розрядні цілі числа: $f(x) = x^{2^{24}+17} + a_1 x^{2^{24}+3} + a_2 x^3 + a_3 x^2 + a_4 x + a_5$ [6].

Мета статті. Відповідно до вищесказаного, мета статті полягає у формуванні на основі теоретичного аналізу методів прикладної криптографії та критеріїв її оцінки, алгоритмів шифрування та криптографії з відкритим ключем, можливість їх застосування і впровадження в системі військового управління з метою засекречування мереж зв'язку військового призначення.

Виклад основного матеріалу дослідження. Для розуміння асиметричного шифрування розглянемо елементи теорії порівнянь [3].

За визначенням $a \equiv b \bmod m$ (читається a порівняно з b за модулем m), якщо a і b дають однаковий залишок при діленні на m, або, іншими словами, $a \equiv b \bmod m$, тоді і тільки тоді, коли $a - b$ ділиться на m без залишку: $m \mid a - b$. Наприклад, $7 \equiv 1 \bmod 6, 6 \mid (7-1)$.

Твердження 1. Якщо $a \equiv b \bmod p$ та $a \equiv b \bmod q$ і p, q – взаємно прості, то $a \equiv b \bmod pq$.

Твердження 2. Якщо $a \equiv b \bmod m$ та $c \equiv d \bmod m$, то $ac \equiv bd \bmod m$.

Якщо так, то з $a \equiv b \bmod m$ витікає $a^s \equiv b^s \bmod m$, де s – будь-який ступінь.

Твердження 3. Якщо $a \equiv b \bmod m$, та $c \equiv d \bmod m$, то $a + c = b + d \bmod m$.

Звідси та з твердження 2 витікає, що в будь-якому арифметичному виразі зі змінних або констант, пов'язаних операціями додавання і множення, можна замість будь-якої величини ставити іншу, з нею порівняну.

Твердження 4. Обидві частини рівняння можна ділити на число *r*, якщо (а) в обох частинах порівняння після ділення залишаться цілі числа; (б) *r* і модуль *m* – взаємно прості.

Доказ. $cr \equiv dr \bmod m \Leftrightarrow m \mid cr - dr \Leftrightarrow m \mid r(c-d)$. У силу (б) $m \mid c-d$, $c \equiv d \bmod m$. Усі дані твердження виводяться з визначення порівняння.

Нам знадобиться ще мала теорема Ферма.

Теорема 1. Якщо *a* не ділиться на просте число *p*, то $a^{p-1} \equiv 1 \bmod p$.

Доказ. Нехай $ar_1, ar_2, \ldots ar_{p-1}$ – повна система обчислень, тобто всі можливі залишки *1, 2...,p-1* при діленні на *p*. Якщо [illegible] не кратно *p*, то числа ar_1, $ar_2, \ldots ar_{p-1}$ всі попарно незрівнянні.

Допустимо від противного, що $ar_1 \equiv ar_2 \bmod p$. Тоді $p \mid ar_1 - ar_2$, тобто $p \mid ar_1 - ar_2$, і оскільки *p* не ділить *a*, то *p* ділить $r_1 - r_2$, тобто $r_1 \equiv r_2 \bmod p$, суперечність. Тоді $ar_1, ar_2, \ldots ar_{p-1}$ теж повна система обчислень, але взята в іншому порядку, тобто за mod *p*

$$\begin{aligned} r_1 &\equiv ar_{i1} \\ r_1 &\equiv ar_{i2} \\ &\ldots\ldots\ldots\ldots \\ r_1 &\equiv ar_{ip-1} \end{aligned}.$$

Перемножуючи ліві частини і праві, отримаємо

$$r_1 r_2 \ldots r_{p-1} \equiv a^{p-1}(r_{i1} r_{i2} \ldots r_{ip-1}) = a^{p-1}(r_1 r_2 \ldots r_{p-1})$$

Оскільки добуток $r_1 r_2 \ldots r_{p-1}$ не ділиться на *p*, можна скорочувати. Отримаємо $a^{p-1} \equiv 1 \bmod p$.

Вироблення секретного ключа по Діффі-Хеллману. Основну роль тут відіграють математичні операції, коли пряма операція порівняно проста, а зворотна – позамежне складна. Такі операції відомі в математиці. З математичних операцій:

1 – легка операція: перемножити два великі числа $P \cdot Q = N$; важка операція: розкласти *N* на множники;

2 – легка операція: піднести підставу a до ступеня *p* і взяти залишок за модулем m: $L = a^p \bmod m$; важка операція: знайти *p*, знаючи *L*, a і m [4].

Обидва важкі завдання загалом вирішуються перебором по *p* і, отже, практично не вирішуються, якщо *p* – дуже велике.

Припустимо, що в комп'ютерній мережі, де відбувається спілкування, загальновідомі основа a і модуль m (це не є попередньою змовою, оскільки a і m можна послати кореспондентові відкритим текстом).

Відправник (s):

Етап 1. Виробляє випадкове число *x, 1<x<m* обчислює $L_s = a^x \bmod m$ і посилає L_s одержувачу.

Етап 2. Отримує L_j обчислює $K_s = L_j^x = a^{xy} \bmod m$.

Одержувач (j):

Отримує L_s, виробляє випадкове число *y, 1<y<m;* обчислює: $L_j = a^y \bmod m$ b і посилає L_j відправникові. Обчислює $K_j = L_s^y = a^{xy} \bmod m$. Через твердження 2 і 3, $K_s = K_j$. Дане число, обчислене як відправником, так і одержувачем, є загальним секретним ключем. Ворог перехопив L_s і L_j, але не зміг дізнатися *x* і *y*.

Приклад. Припустимо $a = 2, m = 601$.

1. Відправник генерує число *x = 178* і посилає одержувачу $L_s = 2^{178} \equiv 8 \bmod 601$. Одержувач генерує *y = 302* і посилає відправникові $L_j = 2^{302} \equiv 4 \bmod 601$.

2. Відправник обчислює $K_s = 4^{178} \equiv 64 \bmod 601$. Одержувач обчислює $K_j = 8^{302} \equiv 64 \bmod 601$.

Система RSA. Відкритими ключами є число *n* (не менше 512 біт) і ключ *e*, що зашифровує [5]. Число *n* є добутком двох простих чисел: $n = pq$, але числа *p* і *q* тримаються в секреті. Секретним є і ключ *d*, що розшифровує. Ключі *d* і *e* задовольняють порівняння $de \equiv 1 \bmod (p-1)(q-1)$. Тепер зрозуміла необхідність тримати в секреті *p* і *q*. Причина в тому, що знаючи *e*, *p* і *q*, можна з останнього порівняння відновити *d*.

Зашифрований текст є послідовністю алфавітно-цифрових символів, скажімо, у коді ASCII; кодам відповідають числа. Таким чином, текст є послідовність тризначних чисел, тобто довге число *m*. Припустимо, що *m*

таке, що $1 \le m \le n$ (текст повинен бути менше ключа, а якщо навпаки, то розіб'ємо текст на менші частини).

Схема передачі повідомлення в системі RSA. Відправник: зашифровує повідомлення m, $1 \le m < n$ так: $c \equiv m^e \bmod n$. Одержувач: розшифровує $m \equiv c^d \bmod n$, $1 \le m < n$. Супостат знає n і e із загальнодоступного довідника, але, перехопивши $c \equiv m^e \bmod n$, він не може відновити повідомлення m, бо надто багато різних m, будучи піднесеними до степеня за модулем n, дають c [5].

Навпаки, одержувач, знаючи d, розшифровує m однозначно.

Приклад. Припустимо, що $n = 3 \cdot 5$, $e = 3$, $d = 3$, $m = 3$, $ed \equiv 1 \bmod 2 \cdot 4$. При зашифровуваній $c \equiv m^e = 3^3 = 27 \equiv 12 \bmod 15$. Отримавши *12*, одержувач проводить розшифровку:

$m = 12^3 = 144 \cdot 12 \equiv 9 \cdot 12 = 108 \bmod 15$.

У загальному випадку справедлива теорема:

Теорема 2. Якщо $n = pq$, $ed \equiv 1 \bmod (p-1)(q-1)$, то m ($1<m<n$; m, n-взаємно прості) володіє властивістю $(m^e)^d = m^{ed} \equiv m \bmod n$.

Доказ. За малою теоремою Ферма $m^{p-1} \equiv 1 \bmod p$. Піднісши обидві частини до степеня *q-1*, отримуємо $m^{(p-1)(q-1)} \equiv 1^{q-1} \bmod p$. Аналогічно (піднісши обидві частини до степеня k) $m^{(p-1)(q-1)k} \equiv 1 \bmod q$. Перемножуючи модулі в останніх двох порівняннях, отримаємо $m^{(p-1)(q-1)} \equiv 1 \bmod pq1$. Поза сумнівом $m \equiv m \bmod n$. Перемножуючи останні два порівняння, отримаємо $m^{(p-1)(q-1)k+1} \equiv m \bmod n$.

З іншого боку,

$ed \equiv 1 \bmod (p-1)(q-1)$, тобто $(p-1)(q-1) \mid ed-1$, тобто ed-1 = k(p-1)(q-1), тобто $ed = (p-1)(q-1)k + 1$.

Це – експонента в лівій частині, яку можна переписати як $m^{ed} \equiv m \bmod n$, що і потрібно було довести.

Щоб зламати шифр *RSA,* необхідно вміти знайти d, для цього досить знайти p і q, які створюють n або, як кажуть, факторизувати n [7]. Основними областями застосування асиметричних алгоритмів шифрування є аутентифікація та обмін ключами. Криптографія з відкритим ключем надає дуже простий спосіб довести, що ви – це саме ви. Припустимо, що *А* і *Б* два користувача системи, а перетворення f_a, яке шифрується, повинен скористатися будь-хто, що відправляє повідомлення користувача *А*, $f_б$ –

відповідне перетворення для користувача *Б*. Для спрощення рахуємо, що множина *P* і *C* елементів відкритого і шифрованого текстів співпадають і однакові у всіх користувачів. Припустимо, що *P* – підпис користувача *A* (що включає інформацію різного роду: особистий номер, ідентифікаційний код тощо). Якщо користувач *A* відправить користувачеві *Б* деяке повідомлення $f_б(P)$, то оскільки способи обчислення $f_б(P)$ загальновідомі, немає способу перевірки, що гарантує, що підпис належить користувачеві *A*. Проте, якщо на початку або кінці повідомлення буде поміщено $f_б f_A^{-1}(P)$, то користувач *Б,* застосувавши $f_б^{-1}$, дешифрує повідомлення, включаючи добавку, і все перетвориться у відкритий текст за винятком добавки, яка набуде вигляду $f_A^{-1}(P)$. Оскільки користувач *Б* знає, що повідомлення повинне було бути послане від користувача *A,* то він застосує до добавки f_A ключ користувача *A,* який йому відомий, і отримає *P*. Оскільки хтось, окрім користувача *A,* не може скористатися функцією f_A^{-1}, зворотною до f_A, то він упевнюється в тому, що повідомлення послане користувачем *A*.

Існуючі криптосистеми з відкритим ключем працюють повільніше, ніж сучасні системи класичного типу. Проте, якщо група користувачів віддає перевагу традиційному типу криптосистем, вона може скористатися криптосхемою з відкритим ключем як допоміжним засобом для розсилки один одному своїх ключів $K = (K_E, K_D)$ для класичної системи.

Висновок. Відмічаємо, що забезпечення ефективного функціонування закритих мереж зв'язку військового призначення та інших інформаційних систем, їх спроможності виконати поставлені завдання з необхідною якістю та у визначені терміни – є ключовим завданням підрозділів зв'язку, які забезпечують процес інформаційного обміну між органами військового управління. Таким чином, можна дотримуватися основного правила класичної криптосистеми і періодично проводити обмін ключами за допомогою порівняльної повільної системи з відкритим ключем, тоді як основний потік повідомлень пересилається з використанням більш швидших колишніх методів.

У **подальшому науковому дослідженні** доцільно на основі теоретичного аналізу інноваційних підходів щодо закриття інформації, застосувавши сучасні інформаційні технології, визначити роль і місце в процесі обміну інформації в системі військового управління та можливості її передавання і зберігання у великих обсягах без уразливості.

Список використаної літератури

1. Стратегічний оборонний бюлетень України : зб. нормат. док. / Рада нац. безпеки і оборони України. – Офіц. вид. // Указ Президента України № 71/2012. – К.: Рада НБОУ, 2012. – 56 с. – (Бібліотека офіційних видань).

2. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке "С" / Б. Шнайер. – М. : Триумф, 2002. – 324 с.

3. Коблиц Н. В. Курс теории чисел и криптографии / Н. В. Коблиц. – М. : НИ ТВП, 2001. – 254.

4. W. Diffie, M.E. Hellman. New directions in cryptography // IEEE Trans. Informat. Theory. – Nov, 1976. –Vol. 1, T-22. – P. 644 -654.

5. D. E. Denning. Digital signatures with RSA and other public-key cryptosystems // Comm. of the ACM, Apr. 1984. – Vol.27. – P. 388–392.

6. Z. Shmuely. Composite Diffie-Hellman public-key generating systems are hard to break // Computer Science Departmant, Technion, Haifa, Israel, Technical Rep. 356, Feb. 1985.

7. Алгоритм RSA: http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1.

8. Алгоритм AES: http://www.nist.gov/aes.

Рецензент – доктор технічних наук,
професор Огороднійчук М. Д.

Стаття надійшла до редакції 04.11.2013.

Розум И. Ю. **Применение прикладной криптографии в системе военного управления в интересах засекречивания сетей связи военного назначения**

В статье рассмотрена возможность применения прикладной криптографии относительно внедрения асимметричных алгоритмов шифровки и криптографии с открытым ключом в системе военного управления с целью засекречивания сетей связи военного назначения.

Ключевые слова: *система военного управления, криптография, засекречивание сетей военной связи, теория сравнений, алгоритмы шифровки.*

Rozum I. Yu. **Implementation of the applied cryptography in the system of military management in interests of classification of military communication networks**

The article there considers the possibility of implementation of the applied cryptography in relation to introduction of asymmetric algorithms of enciphering

and cryptography with open key in the system of military management with the purpose of classification of military communication networks.

Keywords: *system of military management, cryptography, classification of military communication networks, theory of comparisons, algorithms of enciphering.*