Захист інформації

УДК 681.3.06:519.248.681

О.А. Замула

Харківський національний університет радіоелектроніки

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КРИПТОГРАФІЧНИХ СИСТЕМ АБСОЛЮТНОЇ СТІЙКОСТІ

Наводяться необхідні та достатні умови створення абсолютно стійких криптосистем. Обговорюються проблемні питання реалізації таких систем, а також галузі можливого використання криптосистем, що володіють абсолютною стійкістю.

Ключові слова: *криптографічна система, абсолютна стійкість, криптографічний аналіз, ентропія, автентифікація.*

Вступ

На сьогодні використовуються, удосконалюються та розроблюються криптографічні системи (криптосистеми), які забезпечують різноманітний рівень криптостійкості. В ряді джерел [1-2] наведено умови створення криптосистем з різними рівнями стійкості. Проведений аналіз [2] показав, що, якщо в основу класифікації покласти рівень стійкості, то існуючі криптосистеми можна поділити на чотири класи:

1. Криптосистеми абсолютної стійкості (КГС).
2. Розрахунково стійкі криптосистеми.
3. Доказво стійкі криптосистеми (імовірно стійкі).
4. Розрахунково нестійкі криптосистеми (тимчасової стійкості).

Умови та можливості реалізації таких криптосистем залежать від рівня розвитку математичних методів та систем криптоаналізу, тому створення умов і можливостей їх реалізації змінюються з часом. На сьогодні, на наш погляд, вже можна говорити та створювати криптосистеми та засоби, які забезпечують в різноманітних інформаційних технологіях вказані рівні стійкості. Особливо актуальними є задачі створення криптосистем абсолютної стійкості.

Метою статті є розгляд умов та можливостей створення на сучасному етапі розвитку криптосистем абсолютної стійкості.

1. Модель взаємодії користувачів

На рис. 1 наведена спрощена схема інформаційних співвідношень між двома абонентами А1 та А2 (введені такі позначення: 2,9 – пристрої автентифікації; 4,8 – пристрої шифрування; 3, 10 – ключові пристрої; 7 – джерело ключа; 5 – криптоаналітична система (криптоаналітик); 6 – комунікаційна система.

Будемо вважати, що А1 та А2 є джерелами інформації M_i з довільною потужністю алфавіту m та з відомою апріорною статистичною ймовірністю $P(M_i)$ для усіх повідомлень $i = \overline{1, n_m}$ та ентропією джерела інформації $H(M_i)$.

Оскільки повідомлення передається відкритою телекомунікаційною системою, то повинні бути забезпечені конфіденційність та автентичність відповідного рівня. Будемо вважати, що пристрій автентичності забезпечує надання користувачу послуг цілісності та справжності, а пристрій шифрування - послугу конфіденційності.

З метою забезпечення цих послуг використаємо криптоперетворення відповідних класів. Для реалізації криптоперетворень будемо використовувати ключі автентіфікації K_a та ключі шифрування/розшифрування $K_ш$. Також будемо вважати, що ключі генеруються джерелом ключів та використовуються криптографічно стійкі криптопротоколи для розповсюдження ключів абонентам А1 та А2.

Пристрій шифрування здійснює зашифровування або розшифровування повідомлення M_i^a. Будемо вважати відомою статистику появи шифрограми $P(C_i)$ та статистику появи шифрограми $M_i^a - P(C_j / M_i^a)$ після їх зашифрування. При цьому

$$C_j = F_з(M_i^a, K_a, P_r), \qquad (1)$$

де $F_з$ – функція зашифрування, P_r – параметр перетворювання.

Криптоаналітична система, що перехоплює криптограму C_j, має можливість розрахувати апостеріорну статистику $P(M_i^a / C_j)$ – ймовірність того, що C_j, містить в собі M_i^a.

Абонент А2 приймає криптограму C_j^* (знак * означає, що криптограма могла бути випадково або навмисно викривлена).

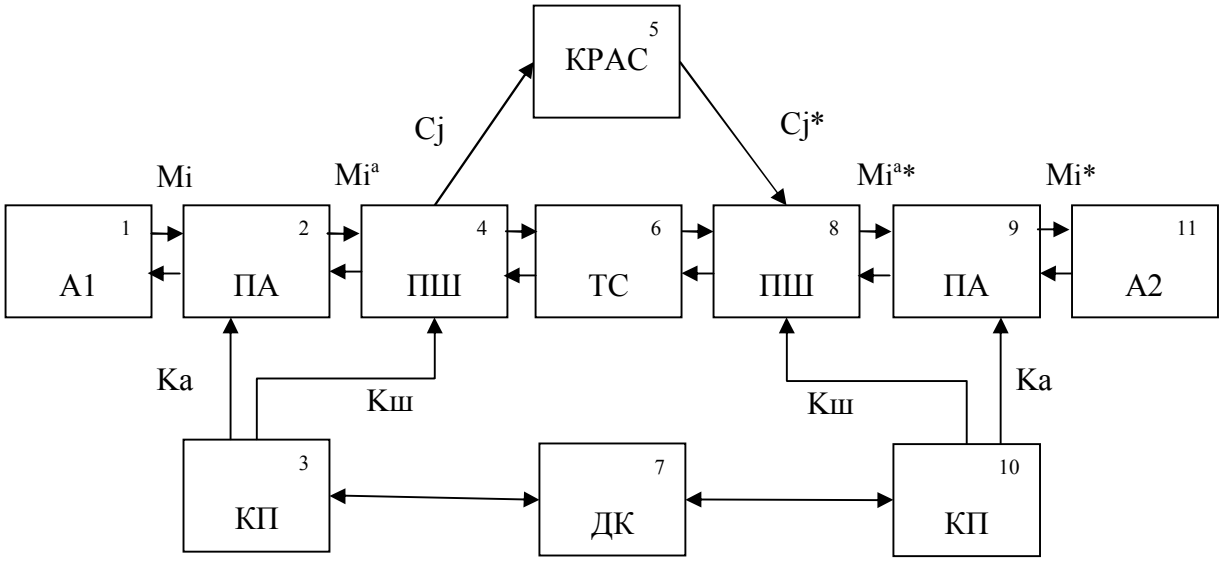

Рис. 1. Спрощена схема інформаційних співвідношень між двома абонентами

Пристрій шифрування 8 здійснює розшифрування даної криптограми, при цьому M_i^{a*} утворюється як

$$M_i^{a*} = F_p(C_j^*, K_ш, P_r), \qquad (2)$$

де F_p – функція розшифрування.

Пристрій автентифікації здійснює криптоперетворення повідомлення M_i^{a*} з метою контролю цілісності та достовірності змісту повідомлення M_i^*. Якщо повідомлення M_i^* достовірне та цілісне, воно видається абоненту А2. При цьому на вхід А2 надходить повідомлення M_i^* і, якщо $M_i^* = M_i$, то ми будемо вважати, що передача здійснена без порушення автентичності та цілісності, а якщо $M_i^* \neq M_i$, то порушена цілісність та автентичність при передачі повідомлення.

Будемо також вважати, що джерело ключів формує на своєму виході ключі K_a та $K_ш$ рівноймовірно, випадково та незалежно з ентропією джерела ключів відповідно $H(K_ш)$ та $H(K_a)$, і що інформаційна система здійснює періодичне передавання криптограм, і криптоаналітик їх перехоплює. Також будемо вважати, що на основі апріорної та апостеріорної статистики криптоаналітик має можливість розраховувати P(M/Cj) для $i = \overline{1, n_m}$ та $j = \overline{1, n_C}$ (n_C - кількість криптограм). При цьому розмірність апостеріорного ряду

$$n_p = n_m \times n_c. \qquad (3)$$

Якщо розмірність ряду, що визначена формулою (3), дуже велика, то практично побудувати або розрахувати ряд неможливо. В зв'язку з цим криптоаналітик повинен вести криптоаналіз з використанням апостеріорної ентропії $H(M_i / C_j)$. При цьому апостеріорна ентропія розраховується згідно співвідношень:

$$H(M_i / C_j) = -\sum P(M_i / C_j) \log_2 P(M_i / C_j), \qquad (4)$$

та

$$H(M_i / C_j) = \sum_j P(C_j) H(M / C_j) = \\ = \sum_{j=1}^{n_c} \sum_{i=1}^{j_{n_m}} P(C_j) P(M_i / C_j) \log_2 P(M_i / C_j). \qquad (5)$$

До початку ведення криптоаналізу криптоаналітик має невизначеність (ентропію) відносно повідомлення

$$H(M) = -\sum_i^{n_m} P(M_i) \log_2 P(M_i). \qquad (6)$$

H(M) отримано при умові, що криптоаналітик знає апріорний ряд $P(M_i)$ (ймовірність появи повідомлення на виході джерела повідомлень). Після перехвату необхідної кількості криптограм невизначеність криптоаналітика відносно джерела повідомлень визначається за формулою (5).

2. Умови реалізації криптосистеми абсолютної стійкості

Розглянемо умови реалізації криптосистеми абсолютної стійкості, використовуючи модель, приведену на рис. 1.

Визначимо, перш за все, яку кількість інформації може отримати криптоаналітик. Умовна ентропія $H(M_i / C_j)$ характеризує невизначеність криптоаналітика після значної кількості отриманих криптограм, причому $H(M_i / C_j)$ характеризує середню невизначеність криптоаналітика відносно джерела

повідомлень. Кількість інформації (ΔI), яку він отримує про джерело повідомлень після проведення криптоаналізу, визначається як

$$\Delta I = H(M) - H(M/C). \qquad (7)$$

При умові, що криптоаналітик не отримує ніякої інформації про джерело повідомлень ($\Delta I = 0$), маємо:

$$H(M) = H(M/C). \qquad (8)$$

Умова (8) і є умовою реалізації криптосистеми абсолютної стійкості. Причому, скільки б шифрограм не перехоплював криптоаналітик, він не збільшить своїх знань про джерело інформації. В цьому випадку криптоаналіз не приводить до успіху.

Криптоаналіз є успішним, якщо $H(M/C) = 0$ і відповідно $\Delta I = H(M)$. В цьому разі кількість інформації, яку отримав криптоаналітик, дорівнює ентропії джерела повідомлення $H(M)$. В більшості криптосистем

$$0 < H(M/C) < H(M). \qquad (9)$$

Співвідношення, що наведено вище, торкається конфіденційності.

Наведемо теорему, яка визначає необхідні та достатні умови реалізації криптосистеми абсолютної стійкості. При цьому зазначимо, що за сучасним поглядом співвідношення (9) є як необхідною, так і достатньою умовою, але воно не визначає практичних методів досягнення мети.

Теорема 1. Необхідною та достатньою умовою забезпечення абсолютної стійкості, схема якої наведена на рис. 1, є наступне

$$P(C_j/M_i) = P(C_j), \qquad (10)$$

тобто ймовірність появи криптограми не повинна залежати ні від того, яке повідомлення вибрано на виході джерела повідомлень, ні від того, який ключ з'явився на виході джерела ключів.

З (10) випливає, що в криптосистемі абсолютної стійкості кожне повідомлення M_i повинно з однаковою ймовірністю відображатися в кожну криптограму. При цьому ми не накладали обмежень ні на потужність алфавіту повідомлення та ключа, ні на довжину повідомлень та криптограм.

Будемо вважати, що джерело повідомлень має алфавіт $m_м$, джерело криптограм - m_c, а довжина повідомлень та криптограм відповідно - l_M та l_C.

Доведення теореми 1. Для доведення теореми розглянемо апостеріорні ймовірності $P(M/C)$ вважаючи, що криптоаналітик перехвачує необхідну йому кількість криптограм. Тобто криптоаналіз відбувається в умовах вибору криптотексту (при відомому криптотексті).

Використовуючи теорему Байєса, $P(C_j/M_i)$ може бути визначена як

$$P(M_i/C_j) = \frac{P(M_i)P(C_j/M_i)}{P(C_j)} = \frac{P(M_i)P(K_{ij})}{\sum_{i=1}^{n_m} P(M_i)P(K_{ij})}. \qquad (11)$$

Відповідно до розглянутого вище співвідношення (8) умовою безумовної стійкості є $H(M) = H(M/C)$. Стосовно до ймовірності появи повідомлення $P(M)$ та апостеріорної ймовірності $P(C_j/M_i)$ можливо записати, що в криптосистемі абсолютної стійкості ймовірність $P(C_j/M_i)$ під час криптоаналізу не повинна змінюватися відносно $P(M_i)$, тобто

$$P(C_j/M_i) = P(M_i). \qquad (12)$$

Інакше, після проведення криптоаналізу, криптоаналітик не отримує будь якої додаткової інформації і його апостеріорні знання не збільшуються відносно джерела інформації для $i = \overline{1, n_m}$ та $j = \overline{1, n_C}$. Розділимо ліву та праву частини співвідношення (11) на $P(M_i) \neq 0$. В результаті маємо

$$\frac{P(M_i/C_j)}{P(M_i)} = \frac{P(C_j/M_i)}{P(C_j)} = 1. \qquad (13)$$

Звідки $P(C_j/M_i) = P(C_j)$. Таким чином умова (10) є як необхідною, так і достатньою.

Вираз (13) фактично означає, що в криптосистемі абсолютної стійкості ймовірність появи криптограми на виході пристрою шифрування не повинна залежати ні від ймовірності появи повідомлень ні від ймовірності появи ключа. Крім того, кількість криптограм повинна бути не менша за кількість повідомлень M_i. Для однозначності дешифрування це означає, що кількість ключів повинна бути не менш за кількість повідомлень, тобто

$$N_K \geq N_M. \qquad (14)$$

З кута зору розглянутого вище інформаційного підходу це означає, що ентропія джерела ключа повинна бути більшою або рівною ентропії джерела повідомлень

$$H(K) \geq H(M). \qquad (15)$$

Для вихідних даних, наведених на рис. 1, кількість повідомлень N_M довжиною l_M при m_M алфавіті є

$$N_M = m_M^{l_M}. \qquad (16)$$

Для ключів з потужністю алфавіту m_K та довжиною l_M

$$N_K = m_K^{l_M}. \qquad (17)$$

Якщо вважати, що всі повідомлення та ключі є равноймовірні, маємо:

$$P(M_i) = \frac{1}{N_M} = m_M^{-l_M}, \qquad (18)$$

$$P(K_j) = \frac{1}{N_K} = m_K^{-l_K}. \quad (19)$$

Відомо, що ентропія джерела ключів (повідомлень) може бути знайдена наступним чином

$$H(K) = -\sum_{i=1}^{N_K} P(K_j)\log_2 P(K_j) = \\ = N_K \frac{1}{N_K}\log_2 \frac{1}{N_K} = \log_2 N_K = \log_2 m_K^{l_K} \quad (20)$$

За аналогією –

$$H(M) = \log_2 m_M^{l_M}. \quad (21)$$

Після підстановки (20) та (21) в (15), отримаємо:

$$\log_2 m_K^{l_K} \geq \log_2 m_M^{l_M}$$

або

$$l_K \log_2 m_K \geq l_M \log_2 m_M.$$

Якщо потужність алфавіту джерела повідомлень та джерела ключів однакова ($m_K = m_M$), а це майже завжди так, то

$$l_K \geq l_M, \quad (22)$$

або

$$l_K = \frac{\log_2 m_M}{\log_2 m_K} l_M. \quad (23)$$

3. Методи реалізації абсолютної стійкості

Проведений аналіз показав, що висунутим вимогам (вибір ключів здійснюється рівноймовірно, випадково та незалежно, а також виконується умова (22)) задовольняє криптосистема відома під назвою «Система Вернама» [3]. В ній зашифрування здійснюється методом потокового криптографічного перетворення за правилом

$$C_i = (M_i + K_i^3) \bmod m. \quad (24)$$

де m – потужність алфавіту C_i; K_i^3 – і-й ключ зашифрування.

Принципова вимога до цього перетворення, це: $l_K \geq l_M$. Розшифрування в такій системі здійснюється за правилом

$$M_i = (C_i - K_i^p) \bmod m, \quad (25)$$

де K_i^p – ключ розшифрування.

Безпосередній аналіз співвідношень (24) та (25) означає, що для розшифрування повідомлення M_i необхідно забезпечити синхронізацію K_i^3 та K_i^p.

Оцінимо стійкість такої системи проти різноманітних криптоаналітичних атак. Оскільки така система має гарантовану стійкість, то при додержанні усіх вищезазначених вимог найкраща атака - це атака типу "брудна сила".

З метою оцінки складності реалізації такої атаки, можна використати показник безпечного часу системи

$$t_б = P_p \frac{N_K}{\gamma K}, \quad (26)$$

де P_p – ймовірність успішного рішення задачі; N_K - кількість ключів; γ - продуктивність аналітичної системи (кількість переборів за секунду); K - коефіцієнт перерахунку, який дорівнює $3.1 * 10^7$ (с/рік)? для отримання значення $t_б$ в роках.

При умові (22) кількість ключів визначається $N_K = m^{l_K}$, а $t_б$ визначається

$$t_б = P_p \frac{N_K}{\gamma K}. \quad (27)$$

Для m=2 (двійковий алфавіт)

$$t_б = P_p \frac{2^{l_K}}{\gamma K}. \quad (28)$$

Для m=*256=2*^{8}

$$t_б = P_p \frac{256^{l_K}}{\gamma K}. \quad (29)$$

В табл. 1 наведено значення $t_б$ для безумовно стійкої криптосистеми, в якій зашифрування та розшифрування здійснюються згідно з правилами (24) та (25). Розрахунки виконано при P_p=1 та $\gamma = 10^{12}$ операцій за сек.

Таблиця 1

Значення $t_б$ для безумовно стійкої систем

довжина, байт	безпечний час системи $t_б$, *років*
8	$1{,}34*10^{-1}$
16	$4{,}17*10^{18}$
32	$2{,}59*10^{57}$
64	$6{,}35*10^{134}$
128	$1{,}63*10^{289}$
256	$5{,}74*10^{597}$
512	$3{,}7*10^{1214}$
1024	$7{,}47*10^{2447}$

Розрахуємо також відстань рівнозначності l_0 для безумовно стійкої криптосистеми.

Відомо, що [1]:

$$H(M/C) = H(K) - l_C r \log_2 m, \quad (30)$$

де H(K) - ентропія джерела ключів; l_C - довжина криптограми; r - збитковість мови; m - потужність алфавіту.

Враховуючи, що криптоаналіз можливий лише за умов H(M/C) = 0, з (30) отримуємо

$$H(K) - l_o r \log_2 m = 0, \quad (31)$$

де l_0 - відстань рівнозначності.

Звідки

$$l_0 = \frac{H(K)}{r \log_2 m}. \qquad (32)$$

Для криптосистеми абсолютної стійкості (правила (24), (25))

$$H(K) = \log_2 N_k = \log_2 2^{l_K} = l_K. \qquad (34)$$

Таким чином:

$$l_0 = \frac{l_K}{r \log_2 m}. \qquad (34)$$

Оскільки, як правило, $r < 1$ (тобто будь яка мова має збитковість), то

$$l_0 > l_K. \qquad (35)$$

Із (35) слідує, що для розкриття шифрограми необхідно, щоб криптоаналітик отримав криптограму довжиною, більшою за довжину ключа.

Таким чином, для реалізації криптосистеми абсолютної стійкості необхідно, щоб довжина ключа була не менш за довжину повідомлення і ключі в системі вибирались би джерелом ключів рівноймовірно, випадково та незалежно.

Висновки

Вище показано, що абсолютна стійкість може бути досягнута при умові, якщо довжина ключа не менша довжини повідомлення, а ключі формуються випадково з рівномірним законом розподілу та є незалежними. Тому першою проблемою, складність якої стримує впровадження криптосистем абсолютної стійкості, є проблема генерування, розповсюдження, установки та використання ключів. Сутність її полягає у виконаній вимоги появлення символів "1" та "0", на різних довжинах ключів з ймовірностями близькими до 0,5. Навіть невеликі відхилення ймовірностей від 0,5 не дозволяють реалізувати безумовну стійкість. Далі, якщо необхідно забезпечити шифрування значних об'ємів інформації, то необхідно розповсюджувати великі об'єми ключів з великою захищеністю від можливою компрометації. При використанні ключів, з однієї сторони необхідно здійснити узгоджене їх використання, в змісті побітової синхронізації, а з другої - їх узгодженого знищення після використання.

Разом з тим, сучасні досягнення у галузі створення та використання носіїв інформації, які можуть бути використані в якості носіїв ключів, роблять можливим розповсюдження та використання ключів. Тому у криптосистемах абсолютної стійкості засоби криптографічного захисту інформації можуть бути реалізовані з використанням навіть звичайних персональних комп'ютерів.

Важливим є забезпечення також цілісності та автентичності ключів, які використовуються. Сутність цієї задачі полягає в тому, що ключі та їх носії повинні бути захищені від порушення цілісності та викривлення. Крім того, навіть в криптосистемах абсолютної стійкості необхідно забезпечити потенційно досяжну автентичність захисту інформації. На наш погляд ця проблема потребує окремого розгляду.

Щодо застосування криптосистем абсолютної стійкості, то вони можуть бути використані для захисту таємної та конфіденційної інформації, ключів різного рівня ієрархії, наприклад, головних ключів (ключів сертифікації та транспортних ключів). При цьому реалізація процедур зашифрування та розшифрування є простою (правила (24) та (25)) і може виконуватись з великою швидкістю.

Метою цієї статі є бажання авторів звернути увагу на можливість реалізації та застосування криптосистем, які забезпечують гарантовану стійкість. Наведені в табл. 1 значення безпечного часу показують, що повідомлення з довжиною 32 байти і більше можуть бути захищені з великою стійкістю.

Список літератури

1. Шеннон К. Теория связи в секретных системах. Работы по теории информации и кибернетике / К. Шеннон. – М.: Изд. иностр. лит., 1963. – 480 с.

2. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: Монографія / І.Д. Горбенко, Ю.І. Горбунко. – Х.: Видавництво «Форт», 2012. – 880 с.

Надійшла до редколегії 15.03.2013

Рецензент: д-р техн. наук, проф. В.А. Краснобаєв, Полтавський національний університет імені Юрія Кондратюка, Полтава.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ АБСОЛЮТНОЙ СТОЙКОСТИ

А.А. Замула

Приводятся необходимые и достаточные условия создания абсолютно стойких криптосистем. Обсуждаются проблемные вопросы реализации таких систем, а также области возможного применения криптосистем, обладающих абсолютной стойкостью.

Ключевые слова: *криптографическая система, абсолютная стойкость, криптографический анализ, энтропия, аутентификация.*

THEORETICAL BASIS OF BUILDING CRYPTOGRAPHIC SYSTEMS OF ABSOLUTE RESISTANCE

A.A. Zamula

Necessary and sufficient terms over of creation of absolutely proof cryptosystem are brought. The problem questions of realization of such systems come into question, and also domains possible application of cryptosystem, possessing absolute firmness.

Keywords: *cryptographic system, absolute resistance, cryptographic analysis, entropy, authentication.*