DOI: 10.18372/2410-7840.19.11767
УДК 004.056

ШВИДКИЙ АЛГОРИТМ ГЕНЕРАЦІЇ ПІДСТАНОВОК БАГАТОАЛФАВІТНОЇ ЗАМІНИ

Геннадій Гулак, Володимир Бурячок, Павло Складанний

В даній статті запропонована актуальна модель порушника кібербезпеки для автоматизованих систем управління технологічними процесами (АСУ ТП), що використовують в якості транспорту глобальні мережі. Виходячи із загроз конфіденційності та цілісності інформації проведено аналіз методів протидії маніпуляціям в мережі і базових методів, що забезпечують перетворення псевдовипадкових послідовностей в послідовності підстановок заміни відповідного ступеня для реалізації шифру багатоалфавітної заміни. В рамках роботи запропоновано швидкий алгоритм реалізації шифру багатоалфавітної заміни з використанням шифрувальної послідовності від блокового шифру в режимі OFB, доведено коректність відповідної процедури та можливість формування будь-якої підстановки з симетричної групи підстановок S_n. Проведено імітаційне моделювання алгоритму, що дозволило підтвердити необхідні статистичні якості матриці перехідних ймовірностей шифру. який забезпечить високий рівень стійкості шифрування та імітостійкість команд і службової інформації, що циркулює в зазначених АСУ ТП.

Ключові слова: *криптологія, шифрування, імітостійкість, метод безповторного набору, підстановочна матриця.*

Вступ. У багатьох автоматизованих системах управління технологічними процесами (АСУ ТП) одночасно постають завдання забезпечення конфіденційності та імітостійкості потоків даних управління та інформації про стан об'єктів, щодо яких здійснюються функції керування. Типові підходи для розв'язку поставлених завдань [1], а саме шифрування за методом гамування, а також формування кодів автентифікації повідомлень (*MAC*) або електронних цифрових підписів можуть суттєво знижувати продуктивність системи управління в цілому та не відповідати форматам подання даних, що підлягають захисту.

У той же час, сучасні стандарти шифрування пропонують режими імітостійкого шифрування у форматі зчеплення блоків (*CBC*) або зворотного зв'язку за шифротекстом (*CFB*), але їх застосування потребує додаткових заходів щодо боротьби із випадковими помилками у каналах зв'язку або застосування спеціальних кодів, що корегують випадкові помилки. Це, в свою чергу, може потребувати додаткових витрат від власника системи, на якого покладається відповідальність за захист інформації в АСУ ТП.

У визначених умовах постає завдання розробити швидкісну криптографічну систему, що забезпечить високу криптографічну стійкість та імітостійкість.

Зазначимо, імітостійкістю (англ. *imitation resistance*) шифру називають його здатність протистояти активним атакам з боку зловмисника, метою якого є нав'язування недійсної інформації шляхом підміни повідомлення, що передається або створення завідомо неприпустимого повідомлення (даних). Фальшиві (недійсні) дані вважаються нав'язаними якщо вони прийняті системою до виконання.

Відносно зловмисника (порушника кібербезпеки)в сучасних умовах доцільно застосувати такі припущення. А саме, зловмисник:

– має необмежений доступ до транспортної мережі;

– може перехоплювати в мережі усі повідомлення що передаються;

– може формувати будь яке нове повідомлення або змінювати на власний розсуд передане повідомлення та надсилати їх у мережу;

– знає достеменно алгоритм шифрування;

– має швидкісну реалізацію алгоритму шифрування, але йому невідомий поточний ключ;

– може виконувати перелічені дії без суттєвої (помітної) затримки.

У визначених умовах вельми ефективним рішенням є застосування різновиду потокових шифрів – шифрів багатоалфавітної (колонної) заміни (БАЗ). При цьому джерелом гами шифру (рис. 1) може виступати надійний блоковий шифр (БШ), який працює у режимі зворотного зв'язку *OFB* й на основі діючого ключа K та вектору ініціалізації IV утворює відповідну псевдовипадкову послідовність (ПВП) [2] - гаму шифру. Гама шифру в подальшому застосовується для формування послідовності підстановок заміни таким чином, що для кожного символу відкритого повідомлення M для отримання чергового символу шифрованого тексту C використовується нова підстановка заміни X.

Зауважимо, що на відміну від шифру гамування, застосування шифру багатоалфавітної заміни забезпечує збереження стійкості криптографічного перетворення навіть у разі повторення ключа шифрування [3].

Сучасна криптологія знає декілька базових методів, що забезпечують перетворення ПВП у послідовність підстановок заміни відповідного степеню для реалізації БАЗ.

Одна група методів базується на доведених властивостях певних підстановок, що полягають у їх здатності у випадку багаторазового множення створювати множини, які співпадають з заданою групою підстановок, у т.ч. симетричною S_n [3]. Проблемою практичного застосування цього методу є складність оперативної заміни системи базових підстановок (утворюючих) та висока складність інженерно-криптографічного аналізу цих реалізацій на предмет виявлення й блокування можливих небезпечних збоїв, помилок та відмов у програмно-апаратній частині криптографічної схеми, які можуть призвести до зниження криптографічних якостей криптосистеми.

Рис. 1. Схема шифрованого зв'язку із застосуванням БАЗ

В деяких застосуваннях для формування підстановок заміни може використовуватися інший спосіб генерації - метод безповторного набору підстановок із випадкової (або псевдовипадкової) рівномірно розподіленої послідовності (РРВП). Суть цього методу полягає у формуванні нижньої стрічки підстановки заміни, використовуючи для цього потік випадкових чисел $j_0, j_1, \dots, j_m, \dots \in \mathbb{Z}_n$ таким чином, що символ, який присутній у сформованій частині стрічки, відхиляється та у подальшому не використовується. Таким чином процес може продовжуватися достатньо довго.

Оскільки у випадку РРВП вибірки з неї є також РРВП, то тільки частина послідовностей одразу без корегування може утворювати нижню стрічку підстановки, тобто.

$$P\left(\begin{pmatrix}0 & \dots & n-1\\ j_0 & & j_{n-1}\end{pmatrix} \in S_n\right) = \frac{|S_n|}{n^n} = \frac{n!}{n^n}. \qquad (1)$$

Для оцінки ймовірності у формулі (1) скористаємось оцінкою Стірлінга для факторіала:

$$P\left(\begin{pmatrix}0 & \dots & n-1\\ j_0 & & j_{n-1}\end{pmatrix} \in S_n\right) \approx \frac{\sqrt{2\pi n}\cdot n^n \cdot e^{-n}}{n^n} = \sqrt{2\pi n}\cdot e^{-n}.$$

Загалом, обсяг вихідних випадкових даних, що необхідні для формування однієї підстановки асимптотично оцінюється величиною $C \cdot n \cdot \ln n$, де C – деяка константа. Практичне застосування цього методу для побудови швидкісних систем управління постає проблематичним.

З урахуванням викладеного постає актуальне завдання розробки швидкісного алгоритму генерації підстановок заміни для БАЗ, що забезпечуватиме конфіденційність та імітостійкість інформаційного обміну в АСУ ТП.

Для опису запропонованого методу генерації підстановок спочатку доведемо наступну лему.

Лема 1. Якщо найбільший спільний дільник чисел $n, \delta \in \mathbb{N}, n > 1$: $(n, \delta) = 1$, то для фіксованого $\forall l \in \mathbb{Z}_n$ у рівнянні

$$l + k \cdot \delta = x_k \bmod n, \qquad (2)$$

для різних $k \in \mathbb{Z}_n$ усі значення $x_k \in \mathbb{Z}_n$ різні.

Доведення. Нехай $k_1 \neq k_2$, але $x_1 = x_2$. Тоді маємо:

$$l + k_1 \cdot \delta = l + k_2 \cdot \delta \bmod n,$$

або:

$$(k_1 - k_2) \cdot \delta = 0 \bmod n.$$

Останнє суперечить вимозі взаємної простоти чисел $(n, \delta) = 1$, тобто $\forall k_1 \neq k_2 \implies x_1 \neq x_2$, що потрібно було довести.

Сформулюємо алгоритм генерації підстановки (АГП) степеню n: $X = \begin{pmatrix} 0 & \dots & n-1 \\ x_0 & \dots & x_{n-1} \end{pmatrix}$ за допомогою послідовності випадкових чисел $j_0, j_1, \dots, j_{n-1} \in \mathbb{Z}_n$.

Для формального опису алгоритму скористаємось оператором Бекуса присвоювання значення деякої змінної: - $\coloneqq$, й позначимо множину сформованих переходів через $\mathcal{A}$.

Послідовність кроків виконання алгоритму наведена у таблиці 1.

Блок схема роботи алгоритму у позначеннях ЕСКД наведена також на рис. 2.

Таблиця 1

Опис алгоритму генерації підстановок

Крок	Формалізований опис	Коментар
1.	$k \coloneqq j_o, m \coloneqq 1,\ \mathcal{A} \coloneqq \{\emptyset\}$.	Ініціалізація змінних.
2.	$x_k \coloneqq j_m$.	Визначення чергового переходу.
3.	$\mathcal{A} \coloneqq \mathcal{A} \cup \{x_k\}$.	Перелік визначених переходів.
4.	$k \coloneqq k + 1 \bmod n$.	Номер наступного переходу.
5.	$m \coloneqq m + 1$.	Номер чергового випадкового числа.
6.	Якщо маємо $m = n$ - виконуємо крок 10, якщо ні – виконуємо крок 7.	Умовний перехід в кінець.
7.	Якщо має місце $j_m \notin \mathcal{A}$ - виконуємо крок 2, якщо ні – виконуємо наступний крок 8.	Умовний перехід до визначення наступного переходу.
8.	$j_m \coloneqq j_m + \delta \bmod n$.	Модифікація випадкового числа.
9.	Далі виконуємо крок 7.	Перехід до перевірки у переліку визначених переходів.
10.	Останньому переходу присвоюємо значення $x_k \coloneqq \mathbb{Z}_n \setminus \mathcal{A}$.	Завершення роботи алгоритму.

Виходячи з леми 1 легко зрозуміти коректність роботи запропонованого алгоритму у сенсі генерації підстановок.

Важливою характеристикою схеми генерації підстановок з точки зору забезпечення необхідних криптографічних якостей шифру багатоалфавітної заміни є: кількість підстановок, що генеруються; ймовірності їх зустрічаємості та матриця перехідних ймовірностей.

Лема 2. Якщо послідовність випадкових чисел $j_0, j_1, \dots, j_{n-1} \in \mathbb{Z}_n$ є незалежною у сукупності та має рівномірний розподіл (РРВП), АГП забезпечує формування S_n - симетричної групи підстановок степеню n.

Цей висновок є достатньо очевидним, оскільки в умовах леми ймовірність появи будь якої послідовності $j_0, j_1, \dots, j_{n-1} \in \mathbb{Z}_n$:

$$P(j_0, j_1, \dots, j_{n-1} \in \mathbb{Z}_n) = \left(1/n\right)^n \neq 0,$$

у тому числі такої, що утворює нижню стрічку підстановки без коригування послідовності.

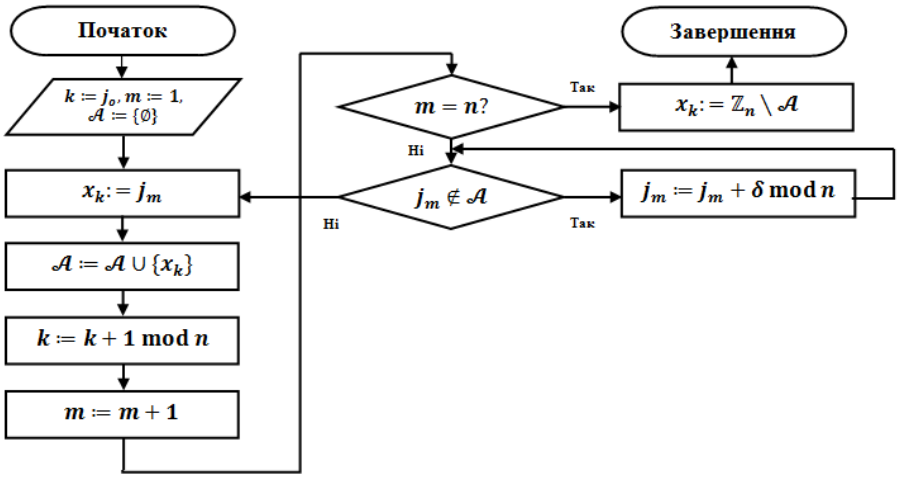

Рис. 2. Блок-схема алгоритму генерації підстановок

Зауважимо, що порівняно з методом безповторного набору запропонований алгоритм завжди виконується за фіксовану кількість кроків, а також він у середньому у $\ln n$ є більш швидким.

Вибір величини n - розміру підстановки заміни – уявляється доцільним здійснювати виходячи з практичних критеріїв «зручності» застосування, забезпечення «достатньої» імітостійкості шифру, а також його швидкодії. Щодо «зручності» застосування можливо відмітити, що для забезпечення зручної реалізації алгоритму доцільно обирати значення, що відповідають розрядній сітці мікропроцесорів, а саме: $n = 2^m$, де $m = 2,4,8,\ldots$ При цьому коефіцієнт імітостійкості БАЗ для $n = 2^2$ є найменшим, а застосування $n = 2^8 = 256$ призведе до суттєвого уповільнення процесу шифрування порівняно з варіантом $n = 2^4 = 16$. Саме такий ступень підстановок заміни пропонується для практичного застосування.

Матриця перехідних ймовірностей для вузла накладання шифру обчислюється за формулою:

$$\mathcal{P} = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix} = \sum_{X_i \in S_n} p_{X_i} \cdot \bar{X}_i, \qquad (3)$$

де $p_{ij} = P(i/j),\ i,j \in \{\overline{1,n}\}$ - умовна ймовірність появи на виході вузла знаку j в разі надходження знаку i; $\bar{X}_i$ – підстановочна матриця, що відповідає генерованої підстановці $X_i \in S_n$.

Враховуючі складний аналітичний вираз для матриці $\mathcal{P}$ було поставлено числовий експеримент, за допомогою якого було з'ясовано що, якщо на вході АГП застосована РРВП, то матриця перехідних ймовірностей $\mathcal{P}$ наближається до рівноймовірної.

У таблиці 2 наведено значення частот елементів статистичного аналога матриці $\mathcal{P}$ для обсягу вхідних даних $N = 5 \cdot 10^3$ для $n = 2^4, \delta = 3$ (для суттєво більшого обсягу даних зменшується наочність подання матриці внаслідок її вельми великого розміру).

Таблиця 2

Статистичний аналог матриці перехідних ймовірностей

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	315	308	307	314	317	313	314	316	313	303	307	302	324	314	325	308
1	313	316	313	314	324	316	311	303	308	312	315	314	314	305	315	307
2	317	312	303	314	319	291	320	317	327	315	300	319	302	317	315	312
3	318	307	318	317	310	304	304	326	313	320	306	317	308	311	313	308
4	315	315	314	310	312	321	309	312	289	304	314	332	307	316	307	323
5	306	308	326	327	312	326	317	310	312	329	308	299	307	300	305	308
6	302	306	323	311	309	308	313	300	319	311	325	308	308	313	323	321
7	305	342	300	317	301	324	314	310	306	317	311	313	309	313	309	309
8	311	308	318	310	305	306	303	328	326	309	309	330	315	318	302	302
9	305	317	324	304	319	345	311	316	311	307	315	290	315	313	303	305
10	308	307	326	307	314	299	307	307	316	316	316	325	317	308	304	323
11	312	315	314	304	314	310	305	300	332	302	317	312	318	311	310	324
12	305	318	306	309	309	312	318	337	304	319	313	318	302	315	311	304
13	337	318	303	305	313	312	313	302	312	304	315	307	315	311	316	317
14	314	304	295	319	314	308	314	308	304	317	314	311	317	323	311	327
15	317	299	310	318	308	305	327	308	308	315	315	303	322	312	331	302

Розподіл зустрічаємості частот у стовпчиках та рядках таблиці перевірявся за допомогою критерію Пірсона χ^2 [4]. Зокрема, для наведених у таблиці 2 даних, значення статистики Пірсона щодо рівномірного розподілу частот у рядках становлять:

Таблиця 3

Значення статистики Пірсона згоди для рядків статистичного аналога матриці $\mathcal{P}$

	Номер рядка															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
χ^2	2,04	1,2	3,99	1,94	4,15	4,49	2,81	4,73	4,03	6,69	2,96	3,15	3,58	3,32	2,91	3,88

Порівнюючи наведені у таблиці 2 значення з квантілем статистики Пірсона з 15 степенями волі з рівнем значущості $\alpha = 0,05$, $\chi^2_{15,0.05} = 25,0$ можливо зробити висновок, що це добре узгоджується з гіпотезою про рівномірний розподіл частот у статистичному аналогу матриці $\mathcal{P}$.

Можливо відмітити, що зі збільшенням обсягу вхідних випадкових даних розподіл частот, що спостерігався у числових експериментах, ще більше наближався до рівномірного.

Підсумовуючи викладене у рамках роботи запропоновано швидкий алгоритм реалізації багатоалфавітного шифру заміни, який забезпечуватиме високий рівень імітостійкості команд та службової інформації, що циркулює в у мережах АСУ ТП й використовує у якості транспорту глобальні мережі.

ЛІТЕРАТУРА

[1] Г. Гулак, В. Мухачев, В. Хорошко, Ю. Яремчук, *Основи криптографічного захисту інформації: підручник,* Вінниця: ВНТУ, 2011, 198 с.

[2] Г. Гулак, Л. Ковальчук "Різні підходи до визначення випадкових послідовностей", *Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні»,* вип. 3, С. 127-133, 2001.

[3] А. Бабаш, Г. Шанкин, *Криптография,* СОЛОН-Р, 2002, 512 с.

[4] С. Айвазян *Прикладна статистика: Основи моделлювання та первинна обробка даних,* М.: Финанси та статистика, 1983, 471 с.

REFERENCES

[1] G. Hulak, V. Mukhachev, V. Khoroshko, Yu. Yaremchuk *Fundamentals of Cryptographic Information Security: Textbook,* Vinnytsya: VNTU, 2011, 198 p.

[2] G. Gulak, L. Kovalchuk "Different approaches to the definition of random sequences" *Scientific and technical collection "Legal, normative and metrological provision of the information security system in Ukraine"*, no. 3, 2001, p. 127-133.

[3] A. Babash, G. Shankin, *Cryptography*, M.: SOLON-R, 2002, 512 p.

[4] S. Ayvazyan, *Applied statistics: Fundamentals of modeling and primary data processing,* Moscow: Finances and Statistics, 1983, 471 p.

БЫСТРЫЙ АЛГОРИТМ ГЕНЕРАЦИИ ПОДСТАНОВОК МНОГОАЛФАВИТНОЙ ЗАМЕНЫ

В данной статье предложена актуальная модель нарушителя кибербезопасности для автоматизированных систем управления технологическими процессами (АСУ ТП), использующих в качестве транспорта глобальные сети. Исходя из угроз конфиденциальности и целостности информации проведен анализ методов противодействия манипуляциям в сети и базовых методов, обеспечивающих преобразование псевдослучайных последовательностей в последовательности подстановок замены соответствующей степени для реализации шифра многоалфавитной замены. В рамках работы предложен быстрый алгоритм реализации шифра многоалфавитной замены с использованием шифрующей последовательности от блочного шифра в режиме OFB, доказано корректность соответствующей процедуры и возможность формирования любой подстановки из симметрической группы подстановок S_n. Проведено имитационное моделирование алгоритма, позволившее подтвердить необходимые статистические качества матрицы переходных вероятностей шифра. который обеспечит высокий уровень стойкости шифрования и имитостойкости команд и служебной информации, циркулирующей в указанных АСУ ТП.

Ключевые слова: криптология, шифрование, имитостойкость, метод безпевторного набора, подстановочная матриця.

FAST ALGORITHM OF GENERATION OF SUBSTATIONS OF MULTIPLE-ALPHABETIC REPLACEMENT

An actual model of the cyber-security offender for automated control systems of the technological processes (APS TP), using global networks as a transport was proposed in this article. Basing on the threats to confidentiality and integrity of information, an analysis of methods of counteracting network manipulation and basic methods were made, that methods ensured the conversion of pseudo-random sequences into substitution sequences of the appropriate degree for the implementation of the multi-alphabetical replacement cipher. Within the framework of the work, a fast algorithm for realizing the multi-alphabetical replacement cipher with the use of the cipher sequence from the block cipher in the OFB mode was proposed, the correctness of the corresponding procedure was proved, and the possibility of forming any substitution from the symmetric permutation group S_n.. The simulation modeling of the algorithm was performed, it allowed to confirm the necessary of the statistical qualities of the matrix of the cipher transition probabilities, which will ensure a high level of encryption and imitation resistance of commands and service information, circulating in the mentioned APS TP.

Keywords: cryptology, encryption, imitostability, a method of non-repetitive typing, substitution matrix.

Гулак Геннадій Миколайович, к.т.н., доцент, Державний університет телекомунікацій.
E-mail: gena.gulak@gmail.com
Гулак Геннадий Николаевич, к.т.н., доцент, Государственный университет телекоммуникаций.
Gulak Gennadii, PhD, Assistant Professor, State University of Telecommunications.

Бурячок Володимир Леонідович, д.т.н., професор, Державний університет телекомунікацій.
E-mail: BVL-home@ua.fm
Бурячок Владимир Леонидович, д.т.н., профессор, Государственный университет телекоммуникаций.
Buryachok Volodymyr, Doctor of technical sciences, professor, State University of Telecommunications.

Складанний Павло Миколайович, аспірант, Державний університет телекомунікацій.
E-mail: p.skladannyi@gmail.com
Складанный Павел Николаевич, аспирант, Государственный университет телекоммуникаций.
Skladannyi Pavlo, graduate student, State University of Telecommunications.