УДК 519.72
Пастернак М. - ст. гр. КН-321
Тернопільський фаховий коледж ТНТУ імені Івана Пулюя

МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ВІЙСЬКОВИХ КОМУНІКАЦІЙ НА ОСНОВІ АЛГОРИТМУ AES-256

Науковий керівник: к.пед.н. Фігурська Л. В

Pasternak M.
Separate Structural Subdivision «Ternopil Professional College of Ternopil Ivan Puluj National Technical University»

MATHEMATICAL FOUNDATIONS OF CRYPTOGRAPHIC PROTECTION OF MILITARY COMMUNICATIONS BASED ON THE AES-256 ALGORITHM

Supervisor**:** PhD in Pedagogy, Liubov V. Fihurska

Ключові слова: криптографія, AES-256, військовий зв'язок
Keywords: cryptography, AES-256, military communications

Постановка проблеми. Захист каналів зв'язку в умовах активного збройного протистояння давно вийшов за межі суто технічного питання. Будь-яке командне повідомлення, перехоплене противником, здатне звести нанівець цілу операцію. Від 2022 року кількість і складність радіоелектронних та кібероперацій них атак проти систем зв'язку ЗСУ зросла на порядок, що зробило проблему криптографічного захисту вже не академічною, а цілком практичною. За таких обставин розробка ефективних механізмів шифрування для тактичних каналів -- це не перспективне завдання, а нагальна необхідність сьогоднішнього дня.

Стандарт AES, затверджений NIST ще 2001 року, тривалий час лишається найпоширенішим алгоритмом симетричного шифрування у світі. За своєю природою AES -- це блочний шифр із розміром блоку 128 біт, який можна розглядати як перетворення векторного простору над полем $GF(2^8)$. Шифрування описується як послідовність нелінійних і лінійних відображень:

$Ek: \{0,1\}^{128} \to \{0,1\}^{128}$, що залежить від ключа k.

Кожен раунд AES реалізує композицію функцій:

- нелінійне відображення S(x) (SubBytes),
- перестановки P(x) (ShiftRows),
- лінійне перетворення L(x) (MixColumns),
- та додавання ключа через XOR: $x_{i+1}=L(P(S(x_i)))\oplus k_i$.

Таким чином AES є ітеративною динамічною системою у дискретному просторі станів.

Практичним наслідком є лавинний ефект, який можна формалізувати як:

$$\frac{\partial Ek(x)}{\partial x} \approx 0.5,$$

що означає зміну приблизно половини вихідних бітів при зміні одного вхідного.

Його варіант із 256-бітним ключем -- AES-256 -- генерує простір ключів 2^{256} комбінацій, що унеможливлює атаку повного перебору навіть при залученні обчислювальних ресурсів квантових систем найближчого горизонту. Армії США та

Великобританії давно інтегрували AES-256 у захищені пристрої зв'язку -- зокрема, класу KG-175 Taclane. Українські силові структури, судячи з доступних відкритих відомостей, рухаються тим самим шляхом, впроваджуючи цей стандарт у комплекси тактичного зв'язку.

У тактичних мережах військового зв’язку передача даних може бути подана як стохастичний процес:

$X(t) \rightarrow Y(t)$, де X(t) -- переданий сигнал, Y(t)-- перехоплений сигнал.

Без шифрування противник намагається оцінити: $P(X|Y)$, але при використанні AES-256 ентропія шифртексту прямує до максимуму:

- $H(Y) \approx Hmax$, що робить відновлення X обчислювально нездійсненним.
- Key rotation можна формалізувати як дискретний процес зміни ключа:
- kt+1=f(kt), що зменшує ймовірність компрометації.

Достатньо порівняти кілька типів комунікаційних систем, щоб оцінити реальну різницю між незахищеним і захищеним зв'язком. Аналогова рація -- найгірший варіант: перехоплений сигнал читається без жодних зусиль. Цифровий зв'язок без шифрування змінює форму сигналу, але не приховує його зміст. AES-256 перетворює корисне навантаження на статистично рівномірний шум -- без знання ключа відрізнити його від випадкового набору байтів неможливо. Захищені супутникові канали йдуть іще далі, ізолюючи метадані і приховуючи сам факт передачі. Ця ієрархія добре ілюструє, чому заміна застарілого аналогового зв'язку на сучасні криптографічно захищені рішення прямо впливає на бойову стійкість підрозділів.

Висновки. AES-256 сьогодні залишається практичним стандартом захисту військових комунікацій -- і підстав для зміни цієї позиції найближчим часом немає. Поєднання стійкого симетричного шифрування, суворої автентифікації та регулярної ротації ключів формує достатній рівень захисту командних і тактичних каналів для поточних умов. Водночас горизонт планування вимагає вже зараз готуватись до постквантової криптографії -- нового покоління алгоритмів, стійких до атак із залученням квантових обчислень. Розробка вітчизняних стандартів шифрування в цьому контексті -- не лише технічне, а й стратегічне завдання.

Список використаних джерел:

1. Daemen J., Rijmen V. The Design of Rijndael: AES The Advanced Encryption Standard. Springer, 2002. 238 p.

2. NIST FIPS PUB 197. Advanced Encryption Standard (AES). National Institute of Standards and Technology, 2001. 51 p.

3. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. Wiley, 1996. 784 p.

4. Бессалов А. В., Телиженко А. Б. Криптосистеми на основі еліптичних кривих. К.: ІВЦ «Видавництво «Політехніка»», 2004. 224 с.