УДК 004.056:004.032:004.9

Живило Євген Олександрович
кандидат наук з державного управління, доцент,
доцент кафедри комп'ютерних та інформаційних технологій і систем навчально-наукового інституту інформаційних технологій та робототехніки Національного університету «Полтавська політехніка імені Юрія Кондратюка»
Кучма Юрій Володимирович
кандидат технічних наук, доцент,
завідувач кафедри комп'ютерних систем ТОВ «Університет сучасних технологій»

ЛІНІЙНА СТРУКТУРА ШИФРУ HILL ЯК ОСНОВА СТАНДАРТУ ШИФРУВАННЯ AES

У роботі досліджується шифр Хілла (Hill cipher) як класичний приклад використання лінійної алгебри та модульної арифметики в криптографічних системах. Алгоритм, запропонований Лестером С. Гіллом у 1929 р. [1] базується на множенні вектора відкритого тексту на ключову матрицю над скінченним полем. Оберненість цієї матриці гарантує можливість відновлення повідомлення, що відображає фундаментальні принципи лінійної криптографії.

Проведений аналіз засвідчив, що Hill cipher став важливою віхою у становленні блокових методів шифрування, які згодом еволюціонували у стандарти **DES** [2] та **AES** [3]. Саме концепція матричних перетворень над полями $GF(2^8)$ у AES відтворює ідею Hill-шифру – лінійне змішування байтів у рамках *MixColumns*, що підвищує лавинний ефект та забезпечує стійкість до статистичного аналізу.

Разом із тим, результати досліджень показують, що Hill cipher є криптографічно нестійким через відсутність нелінійних компонентів. Його лінійність робить алгоритм вразливим до атак із відомим або обраним відкритим текстом [4]. Експериментальні сценарії криптоаналізу демонструють, що ключова матриця може бути повністю відновлена після збору мінімальної кількості пар «відкритий текст – шифротекст», що фактично призводить до повної компрометації шифру.

У межах проведеного аналізу розглянуто три основні категорії атак:

1. Атаки з відомим або обраним відкритим текстом, які дозволяють точно відновити ключову матрицю за кілька ітерацій шифрування;
2. Статистичні атаки на основі лише шифротекстів, що використовують кореляцію частот символів;
3. Атаки побічних каналів, включно з таймінговими та енергоспоживчими [5], які додатково знижують криптостійкість реалізацій.

Виявлено, що головним чинником уразливості є саме лінійна структура перетворення, яка спрощує процес інверсії навіть без повного знання ключа. Це підтверджує, що Hill cipher не відповідає сучасним критеріям безпеки, зокрема вимогам Kerckhoffs-принципу та стійкості до chosen-plaintext attacks.

Попри криптографічну застарілість, шифр Хілла має значну методологічну та дидактичну цінність. Його можна розглядати як навчальну модель, що ілюструє перехід від моноалфавітних систем до блокових алгоритмів і демонструє базові принципи лінійного перетворення у скінченних полях. Цей підхід формує підґрунтя для розуміння внутрішньої структури сучасних стандартів шифрування, таких як AES, які поєднують лінійні та нелінійні операції для досягнення високого рівня криптостійкості [6].

Список використаних джерел

1. Hill, L. S. (1929). Cryptography in an Algebraic Alphabet. *The American Mathematical Monthly, 36* (6), 306–312. https://doi.org/10.2307/2301169.

2. IBM. (1977). *Data Encryption Standard (DES)*. *Federal Information Processing Standards Publication 46*. https://dl.acm.org/doi/10.1145/359168.359172.

3. Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES – The Advanced Encryption Standard*. Springer. https://doi.org/10.1007/3-540-36492-7_1.

4. Stinson, D. R. (2005). *Cryptography: Theory and Practice* (3rd ed.). Chapman & Hall/CRC. https://doi.org/10.1201/9781315370914.

5. Kocher, P., Jaffe, J., & Jun, B. (1999). Differential Power Analysis. In *Advances in Cryptology – CRYPTO' 99* (pp. 388-397). Springer. https://doi.org/10.1007/3-540-48405-1_25.

6. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley. https://doi.org/10.1002/9781118679198.