УДК 004.056.55
Д. Козарик, Ю. Лещишин, к.т.н.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МОДЕЛЮВАННЯ МЕТОДІВ ПОТОКОВОГО ШИФРУВАННЯ ТА ПЕРЕДАВАННЯ ФОТОГРАФІЧНИХ ЗОБРАЖЕНЬ

D. Kozaryk; Yu. Leshchyshyn, Ph.D.

SIMULATION OF STREAM ENCRYPTION METHODS AND TRANSMISSION OF PHOTOGRAPHIC IMAGES

Сучасні засоби цифрового зв'язку для передачі фотографічних зображень, при сучасному розвитку технологій, ґрунтуються на цифрових модемах невеликої потужності та використанні різноманітних методів модуляції. Також їх все частіше використовують у різноманітних портативних та вбудованих комп'ютерних системах для передачі інформації та сигналів керування. З урахуванням необхідності захисту цієї інформації від стороннього втручання, використання криптографічних методів є одним із засобів забезпечення безпеки. Вибір конкретного методу шифрування, будь то симетричний чи асиметричний, залежить від переваг та недоліків, адаптованих до конкретної задачі. Після цього, важливо визначити, як змінюються характеристики системи зв'язку та оцінити її стійкість до завад.

Для побудови систем цифрового зв'язку для передачі фотографічних зображень застосовують мікроконтролери з низьким споживанням енергії та обмеженою обчислювальною потужністю. Таким чином, для цих завдань використовують симетричні алгоритми шифрування, які базуються на єдиному ключі для обох процесів – шифрування та дешифрування (або ключ дешифрування обчислюється за ключем шифрування) [1]. Симетричні алгоритми мають численні переваги, такі як: низькі вимоги до обчислювальної потужності, висока пропускна здатність, короткі ключі та гнучкість використання.

Незважаючи на ці переваги, симетричні алгоритми мають свої недоліки, такі як: складність збереження конфіденційності ключа, велика кількість ключів у розгалуженій мережі та необхідність частої або дистанційної зміни ключів. Проте, у випадку систем цифрового зв'язку, які використовуються в комп'ютерних системах, ці недоліки не є критичними, оскільки час злому таких алгоритмів залишається значною величиною (наприклад, для AES-128 цей час становить 40 років).

Моделюючи системи цифрового зв'язку для передачі фотографічних зображень, можна провести порівняння їх ефективності передачі радіоканалом при використанні різних методів шифрування та без них. Це дозволяє проектувати портативні комп'ютерні системи з високим рівнем захисту інформації використовуючи мінімальні обчислювальні потужності.

Література

1. Whitfield Diffie and Martin Hellman, «Multi-user cryptographic techniques» [Diffie and Hellman, AFIPS Proceedings 45,1976].