УДК 004.056.55:621.39(075)
Ю.З. Лещишин, к.т.н., М.І. Бойко
Тернопільський національний технічний університет імені Івана Пулюя, Україна

МОДЕЛЮВАННЯ МЕТОДІВ СИМЕТРИЧНОГО ШИФРУВАННЯ В ЦИФРОВИХ СИСТЕМАХ ЗВ'ЯЗКУ

Y. Leschyshyn, Ph.D., M. Boyko

SIMULATIONS SYMMETRIC ENCRYPTION IN A DIGITAL COMMUNICATION SYSTEM

Сучасні засоби цифрового зв'язку для портативних пристроїв при теперішньому розвитку технологій базуються на цифрових модемах невеликої потужності із використанням різноманітних методів модуляції. Їх все частіше використовують у різноманітних портативних і побутових пристроях для передачі інформації і сигналів керування. Ця інформація потребує захисту від стороннього втручання. Одним з методів реалізації захисту інформації є використання криптографічних методів. Вибір конкретного методу шифрування (симетричного чи асиметричного) ґрунтується на його перевагах і недоліках стосовно поставленої задачі. Після чого необхідно перевірити – змоделювати як змінились характеристики системи зв'язку та оцінити її завадостійкість.

Зокрема для побудови систем цифрового зв'язку портативних пристроїв використовують мікроконтролери з малим споживанням енергії та невисокою обчислюваною потужністю. Тому для таких задач використовують симетричні алгоритми шифрування які базуються на одному ключі, що використовується для шифрування і дешифрування (або ключ дешифрування обчислюється за ключем шифрування) [1, 2]. Перевагами симетричних алгоритмів шифрування є:

1. Невисокі вимоги до обчислюваної потужності та висока пропускна здатність.
2. Відносно короткі ключі при високій криптостійкості.
3. Гнучкість використання, їх застосовують для створення різних крипто-графічних пристроїв (генераторів чисел, хеш- функції, та ін.)
4. Можливість комбінування методів для підвищення криптостійкості.

Недоліки симетричних алгоритмів шифрування є:

1. Складність збереження конфіденційності ключа.
2. Велика кількість ключів у великій розгалуженій мережі.
3. Необхідність частої або дистанційної зміни ключів.

Для систем цифрового зв'язку, що використовуються в автоматичних пристроях ці недоліки не суттєві, оскільки в більшості випадків перехоплення інформація стає непотрібною при спробі зламу алгоритмічними методами (для AES128 час злому становить 40 років). В таких системах мікроконтролер, що виконує шифрування, є додатковим пристроєм до цифрового модему, тому немає потреби змінювати його конструкцію. Отже при моделюванні до моделі каналу зв'язку із завадами додаються модулі шифрування та дешифрування.

Моделювання таких систем цифрового зв'язку уможливлює порівняння їх ефективності при застосування різних методів шифрування та без них, а отже спроектувати портативні пристрої з високим рівнем захисту інформації.

1. Введение в криптографию; под общ. ред. В. В. Ященко. – СПб.: Питер, 2001. – 288 с.: ил.

2. Романец Ю. В. Защита информации в компьютерных системах и сетях / Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. – М.: Радио и связь, 2001. –376 с.