СКЛАДНОЩІ ТА ПРОБЛЕМИ У РОЗВИТКУ СУЧАСНОЇ КРИПТОГРАФІЇ

Бойко В.Д.

кандидат технічних наук, доцент, доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Пастернак Ю.Ю.

заступник декана факультету кібербезпеки та інформаційних технологій,
асистент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Останні дослідження в області криптографії є важливою інвестицією в майбутнє. Особливо на тлі досягнень сучасного криптоаналізу і постійного зростання обчислювальних потужностей, однак це зростання потужностей має й іншу сторону, більші потужності дозволяють зловмисникам швидше робити атаки грубою силою та вирішувати складніші задачі. Також, незважаючи на те, що криптографія являє собою вже доволі стару науку, вона досі має багато невирішених проблем, кількість яких через технологічний прогрес лише зростає. Через це необхідно постійно розробляти нові криптографічні алгоритми та удосконалювати вже існуючі.

Криптографія та криптоаналіз наразі є найважливішими аспектами розвитку інформаційної безпеки у сучасному світі, а сучасна криптографія зводиться до математичних обчислень, тому, незважаючи на нещодавнє формування сучасної криптографії, вона вже має низку невирішених проблем. Разом із стрімким розвитком технологій та обчислюваних можливостей, збільшуються й можливості зловмисників. Багато алгоритмів, які вважалися алгоритмами з високою крипостійкістю, зараз розкриваються за допомогою атаки брутфорсом. Також враховуючи появу хмарних сервісів та віртуалізації, з'являються зовсім нові вимоги до інформаційної безпеки.

Традиційні алгоритми криптографії були побудовані шляхом поєднання великої кількості простих перетворень, що забезпечує стійкі характеристики кінцевого алгоритму. З тих пір як практичні основи були закладені Горстом Фойстелем, принципи одноключових алгоритмів майже не змінилися. Зміни мали переважно кількісний характер та базувалися на появі більш потужних комп'ютерів. В сучасній криптографії все зовсім по-іншому: надійність алгоритмів базується на недоведеній обчислюваній неможливості ефективного вирішення математичних задач. Наприклад, стійкість RSA криптосистеми базується на складності проблеми факторизації великих чисел, а надійність сучасних схем електронного підпису будується на складності проблеми логарифмування в обмежених полях [3].

Враховуючи це, можна виділити основні сучасні проблеми шифрування:

Обмежена кількість робочих схем. На відміну від класичних алгоритмів криптографії, які можна створювати в необмеженій кількості, комбінуючи різні

елементарні перетворення, сучасні схеми базуються на визначенні «нерозв'язної» проблеми. Як наслідок, ми маємо лише невелику кількість діючих схем з відкритим ключем.

Постійне збільшення розмірів блоків даних та ключів за рахунок розвитку математики та інформатики. Під час розробки RSA криптосистеми, 512-розрядні числа вважалися достатніми, а зараз це не менше 4 Кбіт.

Потенційно ризикова основа. Наразі доведено зв'язок між більшістю обчислюваних проблем, тому у разі якщо одна з сучасних криптосистем буде зламана, то і інші також будуть зламані.

Відсутність далекої перспективи. Передбачуваним кінцем сучасної криптографії є винахід квантового комп'ютеру, хоча поки вони існують лише в теорії.

Сучасні дослідження в сфері криптографії, безумовно, шукають способи вирішення цих проблем. Але криптографічні алгоритми – це лише побудова для створення систем та протоколів. Майже усі відомі вразливості у відомих криптосистемах були пов'язані саме з недоліками проектування та реалізації, тому разом з пошуком та розробкою нових алгоритмів важливу роль також відіграє й якість роботи розробників та проектувальників криптосистем.

Сьогоднішня криптографія повністю побудована на математиці, а головна мета, яку переслідує математика в криптографії це криптографічна стійкість, тобто можливість витримувати теоретичні та практичні атаки на шифр. Таким чином, системи шифрування, які використовуються в криптографічних системах в всесвітній мережі (RSA, ElGamar, Shamir та ін.) використовують останні досягнення теорії чисел та алгебри. Зламати їх – вирішити найскладніші математичні задачі.

Деякі проблеми існуючих криптографічних методів може вирішити, так звана, квантова криптографія. Це відносно новий напрямок досліджень, який дозволяє використовувати ефекти квантової фізики для створення секретних каналів передачі даних. У квантовій криптографії використовується фундаментальна особливість квантових систем, яка полягає в принциповій неможливості точного з'ясування стану такої системи. На сьогоднішній день вже декілька корпорацій пропонують перші комерційні системи квантової криптографії, але самі квантові системи ще не скоро увійдуть у масове використання. Незважаючи на це, квантові системи вже зараз можуть знайти застосування задля захисту особливо важливих каналів зв'язку [4].

Список використаних джерел:

1. Miller V**.** Uses of elliptic curves in cryptography. Advances in Cryptology – CRYPTO'85, Lecture Notes in Computer Science, 218 (1986), pp. 417–426.
2. Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 48 (1987), pp. 203–209.
3. Kahn D. The Codebreakers – The Story of Secret Writing. – Simon and Schuster,1996. – 1200p
4. Fred Cohen A Short History of Cryptography – 1987.