УДК 621.319

ПОРІВНЯЛЬНИЙ АНАЛІЗ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ МЕТОДІВ

Толстова А.В., Голь В.Д., Правило В.В.
Державний заклад Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ», Україна
E-mail: tolstova369@gmail.com

Comparative analysis of cryptographical systems

Comparative analysis of asymmetric cryptographic systems was made. The work algorithms of basic asymmetric cryptographic systems and results of them comparative analysis are presented.

В телекомунікаційних системах розрізняють шифрування повідомлень двох типів: симетричне (із секретним ключем) та асиметричне (з відкритим ключем) [1].

При *симетричному* шифруванні (рис. 1) створюється ключ, файл разом з ключем пропускається через програму шифрування та отриманий результат пересилається адресатові. Ключ передається адресатові окремо, використовуючи інший (захищений) канал зв'язку. Адресат, запустивши ту ж саму шифрувальну програму з отриманим ключем, зможе прочитати повідомлення.

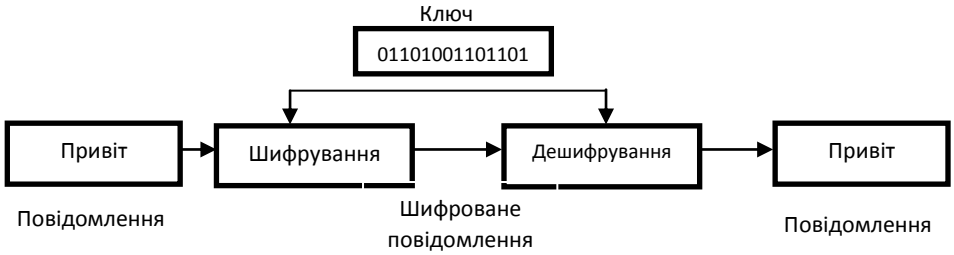

Рис. 1 Симетричне шифрування.

У *асиметричних* криптоалгоритмах (RSA, ElGamal, Diffie-Hellman) (рис. 2) пряме і зворотне перетворення виконуються з використанням відкритого і секретного ключів, що не мають взаємозв'язку, що дозволяє по одному ключу обчислити інший. За допомогою відкритого ключа практично будь-який користувач може зашифрувати своє повідомлення або перевірити електронно-цифровий підпис. Розшифрувати таке повідомлення або поставити підпис може тільки власник секретного ключа. Такі алгоритми дозволяють реалізувати протоколи типу цифрового підпису, забезпечують відкрите поширення ключів і надійну автентифікацію в мережі, стійку навіть до повного перехоплення трафіка [2].

Стійкість ***алгоритму RSA*** базується на складності факторизації великих цілих чисел. Відкритий і закритий ключі є функціями двох великих простих чисел розрядністю 100…200 десяткових цифр і навіть більше. Відновлення відкритого тексту за шифротекстом та відкритим ключем є рівнозначне до розкладання числа на два великі прості множники. Криптоаналіз ані доводить, ані спростовує безпеку алгоритму RSA, тим самим обґрунтовуючи міру довіри щодо алгоритму.

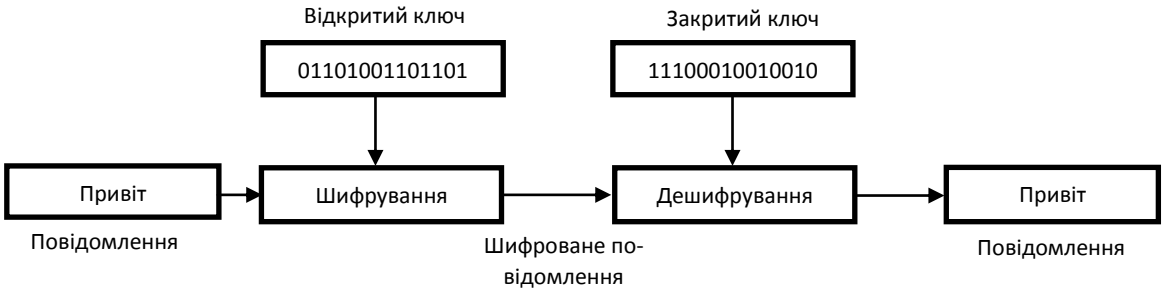

Рис. 2 Несиметричне шифрування.

У довільний спосіб обираються два великі прості числа p та q. Обчислюється добуток $n = pq$. Обчислюється функція Ейлера: $\varphi(n) = (p-1)(q-1)$.

Довільно обирається просте число e – ключ зашифровування, яке задовольняє умовам

$$e < \varphi(n);\ \text{НСД}(e, \varphi(n)) = 1.$$

Обчислюється число d – ключ розшифровування, яке є оберненим до числа e, тобто

$$ed \equiv 1 \pmod{\varphi(n)}.$$

Пара чисел (e, n) є відкритим ключем і розміщується у загальнодоступному довіднику, а числа p, q тримаються у секреті, d – секретний ключ. При шифруванні повідомлення M спочатку розкладається на цифрові блоки, розміри яких менше за n, тобто якщо p та q є 100-розрядними простими числами, то n міститиме близько 200 розрядів і кожен блок повідомлення m_i повинен мати близько 200 розрядів у довжину. Зашифроване повідомлення C складатиметься з блоків c_i такої самої довжини. Формула зашифровування буде мати вигляд:

$$C \equiv M^e \pmod{n}.$$

Розшифровування забезпечується операцією піднесення до степеня d за модулем n одержаного шифртексту C:

$$M \equiv C^d \pmod{n}.$$

Алгоритм Ель-Гамаля є альтернативою алгоритму RSA і при рівному значенні ключа забезпечує таку саму криптостійкість. Безпека алгоритму Ель-Гамаля базується на складності обчислювання дискретних логарифмів. Учасники інформаційного процесу обирають просте число p і ціле число q, який є первинним коренем за модулем p.

Сторона A генерує секретний ключ $k_a < p$ і обчислює відкритий ключ

$$Y_a \equiv q^{k_a} \pmod{p}.$$

Сторона B обирає число $k_b < p$ і за його допомогою зашифровує передаване повідомлення M у такий спосіб:

$$Y_b \equiv q^{k_b} \pmod{p} \quad \text{і} \quad C = M \oplus (Y_a^{k_b} \pmod{p}).$$

Величина M є послідовністю двійкових символів, які передаються до каналу зв'язку. Величина $Y_a^{k_b} \pmod{p}$ перед підсумовуванням перетворюється на послідовність двійкових символів.

Сторона A, отримавши повідомлення у формі Y_b та C, відновлює його:

$$M = (Y_b^{k_a} (\mathrm{mod}\ p)) \oplus C.$$

Алгоритм Діффі-Хеллмана може бути використано задля розподілу ключів (генерування секретного ключа), але його не можна використовувати для шифрування повідомлення.

Згідно алгоритмом Діффі-Хеллмана, учасники інформаційного процесу *A* та *B* домовляються щодо значення великого простого числа *p* і простого дискретного кореня цього числа.

Сторона *A* обирає випадкове число k_a, а сторона *B* – випадкове число k_b у такий спосіб, щоби виконувалися умови

$$1 < k_a < p - 1 \quad \text{та} \quad 1 < k_b < p - 1.$$

Числа k_a та k_b тримаються сторонами *A* та *B* в секреті. Сторони *A* та *B* формують відкриті ключи за правилами

$$Y_{a,b} \equiv a^{k_{a,b}} (\mathrm{mod}\ p).$$

Після обміну несекретними ключами Y_a та Y_b сторони обчислюють значення секретного числа *K*:

$$K \equiv Y_a^{k_b} (\mathrm{mod}\ p) \equiv a^{k_a k_b} (\mathrm{mod}\ p); \quad K \equiv Y_b^{k_a} (\mathrm{mod}\ p) \equiv a^{k_b k_a} (\mathrm{mod}\ p).$$

Здобуте число *K* для ймовірного зловмисника є секретним, оскільки розв'язання рівнянь Y_a та Y_b для великих чисел є неможливе. Алгоритм Діффі–Хеллмана можна поширити на випадок з трьома і більше учасниками [3]. У табл. 1. наведені порівняльні характеристики алгоритмів асиметричного шифрування.

Таблиця 1.

Алгоритм	Ключ	Призначення	Криптостійкість	Примітки
RSA	До 4096 біт	Шифрування та підпис	$2{,}7 \cdot 10^{28}$ для ключа 1300 біт	Заснований на складності задачі факторизації великих чисел. Включений до багатьох стандартів.
ElGamal	До 4096 біт	Шифрування та підпис	При одинаковій довжині ключа криптостійкість рівнозначна RSA, тобто $2{,}7 \cdot 10^{28}$ для ключа 1300 біт	Оснований на складній задачі обчислення дискретних логарифмів в кінцевому полі; дозволяє швидко генерувати ключі без зниження стійкості.
Diffie-Hellman	Рекоменд. 1024 біт	Підпис	Визначається трудністю обчислення дискретного логарифма в кінцевому поле	Базується на передбачуваній складності проблеми дискретного логарифмування; працює тільки на лініях зв'язку, надійно захищених від модифікації

Література

1. Алфьоров А.П., Зубов А.Ю., Кузьмін А.С., Черьомушкін А.В. Основи криптографії: Навчальний посібник. 3-тє вид., Испр. і доп. - М.: 2005. - 480с.
2. Баранов В.М. и др. Защита информации в системах и средствах информатизации и связи. Учебное пособие. – СПб.: 1996. – 111 с.
3. Захарченко М.В. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. / М.В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 184 с.