Криптографічні протоколи блокового-динамічного шифрування

С.М. БІЛАН, І.М. ШВАРЦ

Київського університету економіки і технологій транспорту

A possibility of improving the secret ability of the key transmition channel with the help of the special cryptographic protocol has been considered. An example of a correct exploitation of the protocol during the work of the secret channel has been demonstrated.

Рассмотрена возможность усиления секретности канала передачи ключа за счет разработки специального криптографического протокола. Показан пример правильного использования протокола во время работы секретного канала.

Розглянуто можливість посилення секретності каналу передачі ключа за рахунок розробки спеціального криптографічного протоколу. Показано приклад правильного користування протоколом під час роботи секретного каналу.

Відомо, що для передачі ключа повинен існувати секретний канал. Це також стосується блочних алгоритмів [1]. Блоково-динамічний метод шифрування [2,3] також вимагає наявності секретного каналу й відповідних протоколів передачі ключа з урахуванням несанкціонованого втручання.

У теорії захисту інформації багато уваги приділяється протоколам обміну ключа [4]. Такий протокол повинен підтримувати всі групові операції по видаленню, включенню нових учасників у групу. Передбачається, що учасники групи вже сформували загальний ключ. Розглянемо основні операції, які дозволяють виконувати розроблений протокол. Список операцій, виконуваних протоколом, виглядає так:

- приєднання (JOIN): новий учасник додається в групу;
- злиття (MERGE): один або більше учасників додаються в групу;
- вихід із групи (LEAVE): один або більше учасників залишають групу;
- відновлення ключа (KEY REFRESH): генерація нового ключа для групи.

Для спрощення вважається, що останній учасник групи є контролюючим групи (це не є критичною вимогою і може бути легко виправлено).

Для кращого розуміння зазначимо протокольні терміни та визначення блокового динамічного шифрування.

n - число учасників протоколу;
i, j - індекси для учасників груп;
M_i - і-ий учасник групи;
x_i - довгостроковий секретний ключ M_i;
S_n - груповий ключ n учасників;
$S_n(M_i)$ - внесок M_i -го учасника в груповий ключ;

Для того, щоб запобігти атакам методами підміни або витоку секретних величин, кожний учасник протоколу повинен мати можливість перевірити, що ті значення, які він одержує, є елементами підгрупи. У такому контексті можливості активного супротивника досить обмежені.

Для кращого подання протоколів передачі ключа введемо наступні операції та визначення.

Приєднаннння.

Операція додає нового учасника M_{n+1} до групи з n учасників. Під час операції старий груповий ключ S_n передається по захищеному каналу M_{n+1}, і він стає новим контролюючим групи. Припускаючи, що M_n є поточним контролюючим групи, який передає по захищеному каналу ключ, протокол виглядає в такий спосіб.

1. M_{n+1} виробляє новий секретний ключ x_{i+1}. Потім ключ x_{i+1} розсилається кожному учаснику групи.
2. Після одержання повідомлення від M_{n+1} з новим ключем, користуючись старим ключем, кожний учасник групи $M_i,\ i \in [1,n]$, повідомляє новому учаснику M_{n+1} про те, що він одержав новий ключ.
3. Після одержання повідомлення від кожного учасника групи про те, що він одержав новий ключ x_{i+1} M_{n+1} установлює новий ключ.

Злиття

Операція використовується для додавання $k > 0$ учасників до існуючої групи з $n > 1$ учасників. Нехай $m = n + k$. Під час операції створюється новий груповий ключ S_m, і M_m стає новим контролюючим групи. Припускаючи, що M_n є поточним контролюючим групи, протокол виглядає наступним чином:

1. M_{n+1} створює новий секретний ключ x_{i+1}. Потім він по захисному каналу відправляється до M_i, $i \in [n+2, m]$.
2. Кожний учасник M_j , $j = n+2,\ldots,m$ вже має новий ключ.
3. Потім ключ x_{i+1} розсилається кожному учаснику старої групи $M_i,\ i \in [1,n]$.
4. Після отримання повідомлення M_{n+1} з новим ключем, користуючись старим ключем, кожен учасник групи $M_i,\ i \in [1,n]$, повідомляє M_{n+1} про те, що він одержав новий ключ.
5. Після одержання повідомлення від кожного учасника старої групи $M_i,\ i \in [1,n]$ про те, що він одержав новий ключ x_{i+1}, M_{n+1} встановлює новий ключ.

Операція приєднання також може бути використана для додавання k учасників до групи. Це вимагає повторення операції приєднання k раз, відповідно, через що зростає трудомісткість операції. У такий спосіб для масового додавання учасників групи краще використати операцію злиття. Отже, приєднання використовується для додавання одного учасника до групи, а злиття – для приєднання кількох.

Вихід з групи

Операція виходу із групи видаляє k учасників з n учасників поточної групи. Під час операції обчислюється новий груповий ключ S_{n-k}. M_{n-k} стає новим контро-

люючим групи, якщо M_n залишає групу. Для простоти припустимо, що тільки один учасник M_d виходить зі складу групи. Протокол виглядає наступним чином.

1. M_{n-1} виробляє новий секретний ключ x_{i+1}. Потім x_{n+1} розсилається всім $M_i,\ i \in [1, n-2]$.
2. Після одержання повідомлення M_{n+1} з новим ключем, користуючись старим ключем, кожен учасник групи $M_i,\ i \in [1, n]$, повідомляє M_{n+1} про те, що він одержав новий ключ.
3. Після одержання повідомлення від кожного учасника групи $M_i,\ i \in [1, n-2]$ про те, що він одержав новий ключ x_{i+1}, M_{n-1} встановлює новий ключ.

Учасник M_d не може обчислити новий груповий ключ, тому що контролюючий групи не відсилає йому новий ключ, і при зміні ключа старий учасник не буде мати доступ. Якщо кілька учасників залишають групу, то їм новий ключ не надсилається.

Якщо із групи виходить контролюючий, то вище описані операції виконує передостанній учасник групи M_{n-1}.

Оновлення ключа.

Операція оновлення ключа виконує заміну групового ключа на новий. Ця операція виглядає також, як і операція виходу із групи з k=0, тобто відсилаються нові ключі й після підтвердження всіх учасників про одержання нових ключів ключ змінюється.

Таким чином, з використанням наведених вище операцій досягається повноцінна робота групи.

Між тим, наведена схема роботи не позбавлена недоліків, і найсуттєвіший з них, це, напевно, той, що при додаванні нових учасників групи необхідно використовувати захищений канал. Це прийнятне для невеликих груп, але при великій кількості учасників є доволі складним.

Припустимо, що Оператор1 і Оператор2, що є користувачами комп'ютерної мережі, одержали секретні ключі від Оператора3 (довіреної особи, наділеної правами арбітра). Секретні ключі потрапили до Оператора1 і Оператора2 ще до початку сеансу зв'язку, а зловмисник X нічого не знає про те, які це ключі. Тоді для обміну шифрованими повідомленнями по комп'ютерній мережі Оператор1 і Оператор2 можуть скористатися наступним криптографічним протоколом.

1. Оператор1 зв'язується з Оператором3 і запитує в нього сеансовий ключ для зв'язку з Оператором2.
2. Оператор2 генерує випадковий сеансовий ключ і створює дві шифровані копії цього ключа - один раз Оператор3 шифрує сеансовий ключ за допомогою секретного ключа Оператора1, другий - за допомогою секретного ключа Оператора2. Потім Оператор3 відсилає обидві копії Оператору1.
3. Оператор1 розшифровує свою копію сеансового ключа.
4. Оператор1 відправляє Операторові2 його копію сеансового ключа.
5. Оператор2 розшифровує свою копію сеансового ключа.
6. Оператор1 відправляє Операторові2 повідомлення, зашифроване з використанням сеансового ключа, копія якого є в них обох.

І Оператор1, і Оператор2 повністю покладаються на чесність Оператора3. Якщо Операторові4 вдасться його підкупити або обманути, про таємність обміну повідомленнями між Оператором1 і Оператором2 не може бути й мови. У цьому випадку Оператор4 одержить доступ до всіх ключів, що використовуються абонентами комп'ютерної мережі, і зможе прочитати шифровані повідомлення, якими вони обмінюються по мережі. Для цього Оператору4 досить акуратно скопіювати всю передану через мережу інформацію.

Інший істотний недолік цього протоколу полягає в тому, що арбітр є потенційним вузьким місцем в обміні повідомленнями між Оператором1 і Оператором2. Якщо Оператор3 з якої-небудь причини не зможе вчасно забезпечити їх ключами, шифрований зв'язок між ними буде порушено.

Розподіл відповідальності – це можливість розділення секретного повідомлення на частини, кожна з яких не представляє цінності, але якщо їх певним чином з'єднати разом, знову вийде вихідне повідомлення. Таким чином, пароль ділиться на частини й кожен з колег отримує по однієї його частині, щоб вони змогли розшифрувати дані, тільки зібравшись разом. Зробити це поодинці не зможе жоден з них.

Найпростіший криптографічний протокол дозволяє Операторові3 нарівно розподілити між Оператором1 і Оператором2 відповідальність за збереження повідомлення в таємниці:

1. Оператор3 генерує випадковий бітовий рядок R, що має ту ж довжину, що й вихідне повідомлення M.
2. Оператор3 додає M з R і модулем 2 і одержує S.
3. Оператор3 вручає R Операторові1, а S - Операторові2.

Щоб відновити повідомлення M у первинному вигляді, Оператор1 і Оператор2 повинні спільно виконати останній крок протоколу:

1. Оператор1 і Оператор2 додають R і S за модулем 2 і одержують M.

У вмілих руках даний протокол є досить надійним. Знання S або R не дозволяє реконструювати M. Оператор3 шифрує повідомлення за допомогою одноразового блокнота й віддає отриманий у результаті шифртекст одній людині, а сам блокнот - іншому.

Цей протокол можна легко застосовувати для будь-якого числа учасників. Якщо учасників 4, він буде виглядати в такий спосіб.

1. Оператор3 генерує три випадкових бітових рядки R, S і T, які мають ту ж довжину, що й вихідне повідомлення M.
2. Оператор3 додає M, R, S і T за модулем 2 і одержує U.
3. Оператор3 вручає R Операторові1, S - Операторові2, T - Операторові4, U - Операторові5.

Щоб відновити повідомлення M у вихідному виді, Оператор1, Оператор2, Оператор4 і Оператор5 повинні спільно виконати останній крок протоколу:

1. Оператор1, Оператор2, Оператор4 і Оператор5 додають R, S, T і U за модулем 2 і одержують M.

Одним з учасників протоколу є Оператор3, що наділений необмеженими правами. Наприклад, Оператор3 може зашифрувати яку-небудь нісенітницю замість M, а потім стверджувати, що Оператор1 і інші учасники протоколу оберігають дійсну таємницю, а не якусь нісенітницю. Щоб викрити Оператора3, їм необхідно зібратися разом і відновити вихідне повідомлення. А ще Оператор3 може спочатку роздати частини свого повідомлення Операторові1, Операторові2, Операторові4 і Операторові5, а потім додати M і U за модулем 2 і заявити, що тільки Оператор1, Оператор2 і Опе-

ратор4 потрібні для відновлення повідомлення у вихідному виді, а від Оператора5 можна позбутися. Оскільки повідомлення М цілком належить тільки Операторові3, він може розпоряджатися ним, як того забажає.

Основний недолік криптографічного протоколу, що розподіляє відповідальність за збереження повідомлення в таємниці, полягає в тому, що, якщо хоча б один з його учасників втратить довірену йому частину, буде також назавжди втрачене й саме повідомлення. Якщо, звичайно, Оператор3 не пам'ятає його напам'ять. У результаті в розпорядженні учасників протоколу залишиться тільки довжина вихідного повідомлення. Але навряд чи вони захочуть задовольнятися тільки цим.

Існують ситуації, у яких необхідно вміти відновлювати секретне повідомлення навіть під час відсутності деяких учасників протоколу.

Криптологи придумали так званий граничний протокол, що дозволяє розподіляти відповідальність навіть ще більш складним образом. У загальному випадку береться будь-яке секретне повідомлення (пароль, код запуску балістичних ракет, рецепт готування "Кока-коли") і ділиться на n частин (названих *частками)* так, що для реконструкції вихідного повідомлення обов'язково потрібні m з них. Такий протокол більш точно називається - *граничним* протоколом.

ЛІТЕРАТУРА

1. Александров В.Д., Соколовский Б. Е. Системы защиты коммерческих объектов. Технические средства защиты.- М., 1992, 257 с.
2. С.М. Білан, І.М. Шварц. Вдосконалення алгоритму Blowfish з метою підвищення крипостійкості та швидкодії під час передачі інформації по каналам зв'язку // Реєстрація, зберігання та обробка даних. – 2005. - №1, т.7. С.97-102.
3. С.М. Білан, І.М. Шварц Авторське свідоцтво №12543 „Комп'ютерна програма для передачі інформації по каналах зв'язку з використанням вдосконаленого алгоритму Blowfish (EMailManager)"
4. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь, – 1999, 368 с.

пост. 27.05.05

Моделирование межфазного распределения элементов в системе «металл - шлак» при выплавке стали с наложением низковольтного потенциала

Т.С. СЕМЫКИНА, Д.Н. ТОГОБИЦКАЯ, Л.В. КАМКИНА

Институт черной металлургии НАНУ, Национальная металлургическая академия Украины

На основе физико-химической модели структуры шлакового и металлического расплавов выполнены расчеты на базе экспериментальных данных плавок в 60-т конвертерах по оценке эффективности различных вариантов воздействия электрической энергии на конвертерную ванну по критерию приближения системы «металл - шлак» к равновесию

На основі фізико-хімічної моделі структури шлакового і металевого розплавів виконані розрахунки на базі експериментальних даних плавок у 60-т конвертерах по оцінці ефективності різних варіантів впливу електричної енергії на конвертерну ванну за критерієм наближення системи «метал - шлак» до рівноваги

On the basis of physical and chemical model of frame of slag and metal melts the calculations on the basis of experimental data melts in 60-t converters are executed according to efficiency of different versions of effect of electrical energy on a converter bosh with yardstick of an approaching of a system « metal - slag » to equilibrium

В Институте черной металлургии НАН Украины проводятся работы по нетрадиционному использованию электрических воздействий малой удельной мощности для интенсификации физико-химических, теплофизических и гидродинамических процессов сопровождающих выплавку металла. Одним из разрабатываемых вариантов является применение низковольтных потенциалов при конвертерной плавке. Многочисленные промышленные эксперименты [1-2] убедительно свидетельствуют о существенном улучшении ряда основных показателей процесса выплавки, а также о комплексном характере влияния используемых воздействий. Прежде всего, отмечается ускорение формирования покровного шлака с заданными параметрами и свойствами. В этой связи особый интерес представляет изучение условий передачи подводимой электрической энергии к ванне и характера влияния ее на процессы рафинирования металла от нежелательной примеси.

При этом быстрота протекания реакций между реагирующими фазами определяется различными как внешними, так и внутренними факторами, под влиянием которых система стремится достичь стабильности и к установлению равновесия. Реальные металлургические системы являются неравновесными в виду сложности достижения равновесия, наличия свободного обмена с окружающей средой и футеровкой агрегата, а также прерыванием ионообменных процессов, обусловленным технологическими условиями плавки.

В Институте ведется разработка математических моделей, описывающих физико-химическую структуру шлаковых и металлических расплавов. Проблема многомерности и генерации моделей оптимальной структуры

