для того, чтобы операция была обратимой. По этой причине вместо нуля используется код 65536..

Алгоритм лежащий в основе этого проекта, представляет "объединение операций различных алгебраических групп". Смешиваются три алгебраические группы, и все они могут быть легко реализованы как аппаратно, так и программно: XOR%; сложение по модулю $2^{16} + 1$; умножение по модулю $2^{16} + 1$.

Современные программные реализации IDEA в два раза быстрее, чем DES. На компьютере с i386/33 Mhz IDEA шифрует данные со скоростью 880 Кбит/с, а на компьютере с i486/33 Mhz - со скоростью 2400 Кбит/с. Вы могли бы подумать, что IDEA должен быть побыстрее, но умножение не дешевое удовольствие. Умножение 2-х 32-битовых чисел на процессоре i486 занимает 40 тактов (10 на процессоре Pentium).

Длина ключа IDEA равно 128 битам, а это более чем в два раза больше чем у DES. При условии, что наиболее эффективным является вскрытие грубой силой, для вскрытия ключа потребуется 2^{128} (10^{38}) шифрований. Создайте микросхему, которая может проверять миллиард ключей в секунду, объедините миллиард таких микросхем, и вам потребуется 10^{13} лет для решения проблемы, а это больше чем возраст Вселенной. 10^{24} таких микросхем решат проблему за день, но во Вселенной не найдется столько кремния, чтобы построить такую машину.

Так же алгоритм не поддается взлому путем дифференциального криптоанализа, а также криптоанализа со связанными ключами. В IDEA существует класс слабых ключей, но эти ключи не являются слабыми в том смысле, в котором слабы некоторые ключи DES, для которых функция шифрования обратна самой себе.

ПОРОГОВІ ПРОТОКОЛИ РОЗПОДІЛУ СЕКРЕТУ

Дунь О.В.

Дуже важливою областю криптографії, що інтенсивно розвивається в останні роки, є специфічні протоколи, які одержали назву схем (протоколів) розподілу секрету. По своїй сутності схеми розподілу секрету є

багатосторонніми протоколами, основною функцією яких є установлення ключів або паролів. При цьому під установленням ключів розуміється процес чи прикладний протокол, в результаті виконання якого загальний секрет (ключ, пароль) стає доступним об'єктам чи суб'єктам інформаційної технології, що дозволяє їм виконувати криптографічний захист з необхідною якістю.

Схеми розподілу секрету знайшли також застосування і для сумісного управління критичними технологіями та процесами. В такому управлінні можуть брати участь n об'єктів або суб'єктів. Протокол розподілу секрету складається з двох фаз: фази розподілу секрету та фази відновлення секрету.

Розглядається n учасників протоколу $P_1, \ldots, P_n$, яких ми будемо звати процесорами і один учасник (довірена сторона), якого ми виділяємо і який зветься дилером. На фазі розподілу секрету дилер, який знає деякий секрет S, генерує n часток секрету і посилає S_i частку учаснику P_i по захищеному каналу зв'язку. Також дилер публікує секрет S у зашифрованому вигляді. За допомогою цієї інформації кожний процесор P_n може перевірити, що значення S_i, отримане ним від дилера, дійсно є часткою секрету S. При цьому на S_i накладаються також обмеження, щоб кожні k об'єктів, надавши k справжніх секретів S_i, могли б обчислити загальний секрет $S(k \leq n)$.

На фазі відновлення секрету $k + v$ учасників однозначно відновлюють секрет, обмінюючись повідомленнями по захищених каналах зв'язку, де v з них можуть надати помилковий чи перекручений секрет, а k — справжній, при цьому все одно буде забезпечуватись формування загального секрету. А якщо буде надано $k - 1$ приватних секретів, відновити S буде неможливо (безумовно чи за допомогою обчислення).

ПОТЕНЦИАЛ ИСПОЛЬЗОВАНИЯ INTERNET-СТРАТЕГИИ CRM

Остривная Л.Г.

Сейчас руководители информационных служб все чаще сталкиваются в своей практике с так называемым управлением отношениями с