АНАЛИЗ АЛГОРИТМОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Волынец С. В.

Давыденко И. Н. – канд. техн. наук, доц.

Приведен сравнительный анализ современных алгоритмов криптографической защиты информации.

В эпоху бурного развития технологий, проблемы информационной защиты встают наиболее остро. Использование автоматизированных систем обработки информации и управления упростило защиту информации, от несанкционированного доступа. Основные проблемы защиты информации в компьютерных системах возникают из-за того, что информация не является жёстко связанной с носителем. Её можно легко и быстро скопировать и передать по каналам связи. Информационная система подвержена как внешним, так и внутренним угрозам со стороны нарушителей.

Решение проблем защиты электронной информации базируется в основном на использовании криптографических методов. Притом современные методы криптографического преобразования сохраняют исходную производительность автоматизированной системы, что является немаловажным. Это является наиболее эффективным способом, обеспечивающим конфиденциальность данных, их целостность и подлинность. Использование криптографических методов в совокупности с техническими и организационными мероприятиями обеспечивают надежную защиту от широкого спектра угроз.

С целью установления подлинности источника информации либо аутентификации получателя используется такое средство защиты информации как электронная цифровая подпись (ЭЦП). Механизм осуществления ЭЦП строится на основе асимметричных криптоалгоритмов и заключает в том, что для шифрования сообщения используется один ключ, а при дешифровании - другой. Кроме того, процедура шифрования выбрана так, что она необратима даже по известному ключу шифрования.

В теории криптографии разработаны требования к асимметричным криптосистемам, которые полностью покрывают требования предъявляемые к модулям разрабатываемой системы:

– вычисление пары ключей (КА, КВ) получателем В на основе начального условия должно быть простым;

– отправитель А, зная открытый ключ КА и сообщение М, может легко вычислить криптограмму С:

$$C = E_{K_A}(M) = E_A(M);$$

– получатель В, используя секретный ключ КВ и криптограмму С, может легко восстановить исходное сообщение М:

$$M = D_{K_B}(C) = D_B(C) = D_B[E_A(M)];$$

– злоумышленник, зная открытый ключ КА, при попытке вычислить секретный ключ КВ наталкивается на непреодолимую вычислительную проблему;

– злоумышленник, зная пару (КА, С), при попытке вычислить исходное сообщение М наталкивается на непреодолимую вычислительную проблему.

В докладе приведен сравнительный анализ эффективности методов криптографической защиты информации, произведено сравнение алгоритмов защиты по основным параметрам с целью определения наиболее оптимального. В качестве основных рассматриваемых методов криптозащиты выбраны алгоритмы потокового шифрования данных с открытым ключом RSA, ElGamal, DSA и ECDSA.

Алгоритм RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) основывается на вычислительной сложности задачи факторизации больших целых чисел. Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других.

Elgamal (Эль-Гамаль) – криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамаля лежит в основе стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).

Алгоритм ECDSA аналогичный по своему строению DSA, но определённый в отличие от него не над полем целых чисел, а в группе точек эллиптической кривой. Применение метода эллиптических кривых дает возможность работы на значительно меньших полях Галуа по сравнению с алгоритмом DSA. Как, в общем, с криптографией эллиптической кривой, предполагается, что битовый размер открытого ключа, который будет необходим для ECDSA, равен двойному размеру секретного ключа в битах. Для сравнения, при уровне безопасности в 80 бит (то есть атакующему необходимо примерно 2^{80} версий подписи для нахождения секретного ключа), размер открытого ключа DSA равен, по крайней мере, 1024 бит, в то время как открытого ключа ECDSA – 160 бит. С другой стороны размер подписи одинаков и для DSA, и для ECDSA: 4t бит, где t – уровень безопасности, измеренный в битах, то есть – примерно 320 бит для уровня безопасности в 80 бит.

Развитие алгоритмов, основанных на методе работы с эллиптическими кривыми, являются перспективным направлением криптографической защиты информации.