УДК 512.624.95:378.147.091.3

О модификации Шнорра криптосистемы Эль Гамаля

Крупенкова Т.Г., Липницкий В.А.
Белорусский национальный технический университет,
Военная академия Республики Беларусь

Криптографическая система Эль Гамаля появилась в 1985 году как освежающая реакция на излишнюю сложность криптосистемы RSA. В основе реальных криптосистем Эль Гамаля лежит большое простое число $p \approx 2^{1024}$. Предполагается, что в разложении $p-1 = \prod p_i^{r_i}$ имеется простой множитель $q \approx 2^{160}$. В поле $Z/\mathrm{p}Z$ имеется элемент g порядка q. Числа p, g, h образуют тройку открытых ключей криптосистемы Эль Гамаля. Здесь $h \equiv g^x (\mathrm{mod}\, p)$; x – секретный ключ, некоторое целое число, известное только составителю и адресату (идея Питера Шнорра). Отправитель генерирует ещё один, известный только ему, секретный ключ k. Сообщения c шифруется по правилу: $ш = cK (\mathrm{mod}\, P)$. где $K \equiv h^k (\mathrm{mod}\, p)$. Как в хорошем детективе, шифровка сопровождается подсказкой для возможных хакеров – числом $h \equiv g^x (\mathrm{mod}\, p)$.

Для расшифровки достаточно знание чисел $p, ш, O_{sk}, x$. Остальной магический калейдоскоп нужен только для того, чтобы направить хакеров по единственному руслу – решению проблемы дискретного логарифма – поиску степени x в равенстве $h \equiv g^x (\mathrm{mod}\, p)$, причем единственным известным на то время методом – «baby step».

В 2005 году неожиданно вскрылось существование метода «baby step giant step», секретно созданного ещё в 1962 году Шэнксом Д., что существенно подорвало доверие к криптосистеме. Криптографический стандарт DES спасло на долгие годы трёхкратное увеличение ключа. Аналогично предлагаем многократно увеличить диапазон изменения x, заменив g на образующую всей мультипликативной группы $Z/\mathrm{p}Z^*$ поля $Z/\mathrm{p}Z$ (что также снимет исходные ограничения на p), а не её примитивной во всех отношениях подгруппы порядка q, которую услужливо, но абсолютно незаслуженно, начинают называть группой Шнорра – явный курьёз современной истории развития науки.