Кондачков Е.Д. 5151004/90101

Резюме по статье «Fast Variants of RSA»

В своей работе авторы статьи отмечают значимость и распространенность криптосистемы RSA, а также её главный недостаток – недостаточно быструю работу. В статье предлагается 4 варианта решения это проблемы, причем все варианты являются обратно совместимыми, то есть способными взаимодействовать со стандартной реализацией RSA.

Batch RSA или «пакетный» RSA – модификация стандартного алгоритма, при котором можно расшифровать два шифртекста примерно по цене одного, при условии что в открытых ключах (n_1, e_1) и (n_2, e_2) $n_1 = n_2$, а e_1 и e_2 малы. Для этого нужно вычислить $C_1^{\frac{1}{e_1}} mod\ N\ C_2^{\frac{1}{e_2}} mod\ N$, но данную операцию можно привести к виду $A = (C_1^{e_2} * C_2^{e_2})^{1/(e_1 * e_2)}$, что позволяет уменьшить количество операций взятия корня до одной. Данный способ позволяет достичь увеличения скорости до 3 раз, но требует очень маленьких открытых показателей ($e = 3,5,7,11, \dots$)

Вторая модификация – Multi-prime RSA или RSA с несколькими простыми. Основная суть данной модификации заключается в использовании вместо двух больших простых чисел b простых чисел меньшей размерности. Прирост производительности осуществляется за счет снижения сложности операции возведения в степень по модулю. Так, в классической реализации используется возведение в степень по модулю $\frac{n}{2}$-разрядных чисел. В данной модификации берется модуль по модулю $\frac{n}{b}$-разрядных чисел. Данное нововведение дает прирост производительности в 2 и более раз, в зависимости от n. Стоит отметить, что в случае 1024-разрядного n простых чисел в целях безопасности можно взять только 3, то есть pqr.

Третья модификация схожа со второй, и относится к той же группе. Multi-factor RSA или RSA с несколькими степенями. Суть модификации идентична предыдущей, но в данном варианте выбирается не b различных простых чисел длины $\frac{n}{b}$, а p и q, причем p берется $b - 1$ раз, то есть $n = p^{b-1}q$.

Таким образом дешифрования требует двух возведений в степень по модулю $\frac{n}{b}-$ битных чисел и $b-2$ поднятий Хензеля. Данный способ дает прирост производительности примерно в 3 раза.

Последней модификацией является Rebalanced RSA или перебалансированный RSA. Основная идея данной модификации состоит в уменьшении времени дешифрования за счет увеличения времени шифрования. В данном методе d выбирается так, чтобы оно было порядка n, но при том $d(mod\, p-1)$ и $d(mod\, q-1)$ были малыми числами. Это позволяет в КТО заменить показатель на k-разрядные числа, где k сравнительно мало. Прирост производительности при таком подходе порядка 3 раз.