16 Специальное умножение

Задача. В стандарте ЭЦП Узбекистана O'z Dst 1092:2009 (`http://pki.uz/downloads/standarts/OzDSt_1092_2009.pdf`) используется специальное умножение

$$x \circledR y = x + (1 + xR)y \bmod p,$$

где p — простой модуль, R — произвольный вычет по этому модулю. Покажите, как можно найти 100-ую степень x относительно операции ®, использовав не более десяти умножений и двух сложений / вычитаний по модулю p. Разрешается проводить предвычисления с p и R.

Решение. Пусть $\varphi(x) = xR + 1$ (здесь и далее предполагаем, что арифметические вычисления выполняются по модулю p). Тогда

$$x \circledR y = \varphi^{-1}(\varphi(x) \cdot \varphi(y)),$$

где «$\cdot$» — обычное умножение, $\varphi^{-1}(z) = (z - 1)R^{-1}$.

Понятно, что

$$x \circledR x = \varphi^{-1}((xR + 1)^2), \quad x \circledR x \circledR x = \varphi^{-1}((xR + 1)^3)$$

и так далее. В частности, 100-ая степень x относительно ® есть

$$((xR + 1)^{100} - 1)R^{-1}.$$

Для определения 100-й степени можно предварительно рассчитать R^{-1} (расширенный алгоритм Евклида) и организовать вычисления следующим образом:

1) найти $z = xR + 1$ (1 умножение и 1 сложение);

2) найти $z^2, z^4 = (z^2)^2, \ldots, z^{64} = (z^{32})^2$ (6 умножений);

3) найти $z^{100} = z^{64} \cdot z^{32} \cdot z^4$ (2 умножения);

4) найти $(z^{100} - 1)R^{-1}$ (1 вычитание и 1 умножение).

Насколько мы поняли, специальное умножение введено в O'z Dst 1092:2009 для того, чтобы была возможность создавать группы привилегированных абонентов. Действительно, если параметр R известен только определенным абонентам, то только эти абоненты могут проверять подписи друг друга.

Интересный вопрос: насколько сложной является задача определения R по открытым ключам и подписям привилегированных абонентов?

□