Sławomir Górawski

Lista 6, zadanie 6. Alicja chce przesłać tę samą wiadomość m do Boba, Charliego i Davida za pomocą kryptosystemu RSA. Załóżmy, że $e_B = e_C = e_D = 3$ dla różnych n_B, n_C, n_D. Pokaż, jak Oskar może odszyfrować wiadomość m po przechwyceniu jej szyfrogramów.

Rozwiązanie. Niech c_B, c_C, c_D będą szyfrogramami, a $x = m^3$. Wtedy:

$$\begin{aligned} x &\equiv c_B \mod n_B \\ x &\equiv c_C \mod n_C \\ x &\equiv c_D \mod n_D \end{aligned}$$

Załóżmy, że n_B, n_C, n_D są względnie pierwsze. Wtedy możemy znaleźć wartość x, która to spełnia, przy użyciu chińskiego twierdzenia o resztach. Z twierdzenia tego wynika, że wszystkie rozwiązania przystają do siebie modulo $N = n_B n_C n_D$. Weźmy najmniejsze możliwe x (powinniśmy byli znaleźć właśnie takie, a jeśli nie, to weźmy x modulo N). W RSA m musi być mniejsze niż n_B, n_C i n_D. Mamy $x \equiv m^3 \mod N$, gdzie $x < N$ oraz $m^3 < N$. W takim razie $m = \sqrt[3]{x}$.