Sławomir Górawski

Lista 6, zadanie 3. Alicja chce przesłać tę samą wiadomość m do Boba i Charliego za pomocą kryptosystemu RSA. Bob i Charlie używają tego samego n, ale różnych wykładników klucza jawnego e_B i e_C. Załóżmy ponadto, że $\gcd(e_B, e_C) = 1$. Pokaż, jak Oskar może odszyfrować wiadomość m po przechwyceniu jej szyfrogramów przeznaczonych dla Boba i Charliego. Czy daje to mu możliwość odtworzenia kluczy deszyfrujących?

Rozwiązanie. Niech c_B i c_C będą przechwyconymi szyfrogamami. Wiemy, że:

$$m^{e_B} \equiv c_B \mod n,$$
$$m^{e_C} \equiv c_C \mod n.$$

Używając rozszerzonego algorytmu Euklidesa, możemy znaleźć takie s_B i s_C że:

$$e_B s_B + e_C s_C = \gcd(e_B, e_C) = 1.$$

Wtedy możemy odszyfrować wiadomość m w następujący sposób:

$$c_B^{s_B} \cdot c_C^{s_C} \equiv m^{e_B s_B} \cdot m^{e_C s_C} \equiv m \mod n.$$

Jedna z liczb s_B, s_C jest ujemna (załóżmy że s_C), więc w praktyce chcemy policzyć:

$$(c_C^{-1})^{-s_C} \mod n,$$

co wymusza dodatkowe założenie, że $\gcd(c_C, n) = 1$. Czy daje to możliwość odtworzenia kluczy deszyfrujących? Nie, aby mieć taką możliwość, Oskar musiałby otrzymać wiadomość m zaszyfrowaną tym samym n oraz wykładnikiem e_O, dla którego znany jest mu klucz deszyfrujący d_O. Wtedy mógłby rozłożyć n i znaleźć d_B oraz d_C. Bez tego jednak nie dysponuje żadną informacją, która mogłaby nam ułatwić odtworzenie kluczy deszyfrujących.