RSA – matematyka dyskretna

Na podstawie skryptu

Algorytm szyfrowania wiadomości w blokach jednoznakowych, dla alfabetu 32 znakowego:

Σ = { a, b, c, d, e ,f , g, h……}

1. Aby coś zaszyfrować musimy przede wszystkim ustalić liczbę „n", która musi być iloczynem dwóch liczb pierwszych, jednocześnie musi być większa od mocy zbioru Σ[1] np.:
   n = 3 * 11 = 33
2. Następnie ustalamy liczbę „ϕ(n)", która jest równa iloczynowi liczb pierwszych ,wcześniej użytych do ustalenia n, zmniejszonych o 1. W naszym przypadku:
   ϕ (n)= (3-1) * (11-1) = 20
3. Teraz należy wybrać liczbę „e" – wykładnik szyfrujący, względnie pierwszą z ϕ (n) (liczby względnie pierwsze to takie , które niekoniecznie są pierwsze, ale nie maja wspólnych dzielników różnych od 1). Wybierzemy liczbę 7.
   e = 7
4. Gdy mamy wykładnik szyfrujący, potrzebujemy znaleźć także wykładnik deszyfrujący – „d" (d Є N) , iloczyn wykładników musi być równy 1 w „modulo ϕ(n)":
   d * e = 1 (mod ϕ(n)), dla naszego przypadku
   d * 7 = 1 (mod 20), liczbę d znajdziemy za pomocą rozszerzonego algorytmu Euklidesa[2]
   d= 3
5. Aby wysłać zaszyfrowaną wiadomość (w jednoelementowym bloku – 1 literę) wybieramy ją z naszego pseudo-alfabetu, w naszym przykładzie wybieramy literę „b", odpowiadający jej kod z naszego alfabetu to 2 (A-1 B-2 C-3 ….). Podnosimy ją do potęgi „e" (modulo n)i wysyłamy odbiorcy znającemu „n" i „d":
   $2^e = 2^7 = 128 \text{ (mod 30)} = 8$
6. Osoba znająca klucz prywatny („n" i „d"), podnosi wiadomość do potęgi „d" (modulo n) i otrzymuje pierwotną wiadomość:
   $$8^3 = 64 * 8 \ (mod\ 30) = 4 * 8 = 32 \ (mod\ 30) = 2$$
   2 – B, odbiorca dobrze odszyfrował wiadomość.

[1] Dla wysyłania wiadomości w blokach x-elementowych liczba „n" musi być większa niż moc zbioru Σ podniesiona do potęgi x
$n>|\Sigma|^x$

[2] Jego opis znajdzie się w następnym pdfie