Szyfrowanie RSA

Wiktoria Kubik, Marta Rzekanowska
Koordynator: Ola Puchała

1. Wstęp

Głównym celem kryptografii jest szyfrowanie informacji w taki sposób, aby osoby nieuprawnione nie mogły ich odczytać. Jednym ze sposobów na to jest szyfrowanie RSA, którego zrozumienie było celem naszego projektu.

2. Potrzebne zagadnienia

• Elementy odwracalne

Załóżmy, że $n \geq 2$ oraz $a, b \in \mathbb{Z}$.
Mówimy, że a jest elementem odwrotnym b, gdy $a \cdot b \equiv 1 \mod n$.
Wówczas element a jest odwracalny, a jego odwrotność oznaczamy a^{-1}.

• Twierdzenie Eulera

Jeśli a jest liczbą całkowitą względnie pierwszą z $n \geqslant 2$, to

$$a^{\varphi(n)} \equiv 1 \mod n$$

• Funkcja Eulera

$\varphi(n)$ to ilość elementów odwracalnych w pierścieniu $\mathbb{Z}_n$.

• Małe twierdzenie Fermata

Jeśli a jest niezerową liczbą całkowitą i p jest liczbą pierwszą, to:

$$a^{p-1} \equiv 1 \mod p$$

3. Działanie RSA

• Szyfrowanie

- Wybieramy dwie bardzo duże liczby pierwsze p i q.
- Ustalamy $N = p \cdot q$.
- Obliczamy $\varphi(N) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$.
- Wybieramy dowolne e, takie że $1 < e < \varphi(N)$.
- Para (N, e) to nasz **klucz publiczny**.
- Wyznaczamy d - odwrotność modularną liczby e:
$$d = e^{-1} \mod \varphi(N).$$
- Para (N, d) to nasz **klucz prywatny**.
- Wiadomość, którą chcemy przesłać (zamienioną na wartość liczbową) będziemy oznaczać jako M.
- Teraz definiujemy naszą funkcję szyfrującą:
$$D(M) = M^d \mod \varphi(N)$$
i funkcję deszyfrującą:
$$E(M) = M^e \mod \varphi(N).$$

• Dlaczego działa?

Każdy ma dostęp do naszego klucza publicznego, jednak aby mieć nasz klucz prywatny niezbędny do odszyfrowania wiadomości, musi obliczyć d, a do tego potrzebuje znać wartość $\varphi(N)$.
I tutaj pojawia się problem włamywacza, gdyż jedynym sposobem na poznanie tej wartości jest faktoryzacja naszej liczby N i otrzymanie p i q.
Jest to jednak zadanie trudne nawet dla komputera, bo operujemy na bardzo dużych liczbach.

4. Skuteczność

• RSA na co dzień

Obecna technologia nie pozwala na faktoryzację tak ogromnych liczb jak N, w rozsądnym czasie co sprawia, że szyfrowanie RSA pozostaje bardzo skutecznym sposobem ochrony informacji. Największym kluczem, który dotychczas został złamany miał 250 cyfr w systemie dziesiętnym[1]. Szacuje się, że aby złamać klucz o długości 617 cyfr potrzeba około 300 bilionów lat[2].

• A gdzie jest haczyk?

Możliwe, że w przyszłości faktoryzacja dużych liczb będzie możliwa z wykorzystaniem algorytmu Shora zaprojektowanego dla komputerów kwantowych.

5. Podsumowanie

Szyfrowanie RSA pomimo swojej względnej prostoty jest bardzo ciężkim do złamania szyfrem, co zapewnia obecnie wysokie bezpieczeństwo przechowywanych informacji. Niestety wraz z rozwojem technologii będzie można na nim coraz mniej polegać.

Bibliografia:
[1] Zimmermann, Paul: "Factorization of RSA-250".
[2] Johnson, James: "The Vulnerabilities to the RSA Algorithm and Future Alternative Algorithms to Improve Security".
[3] en.wikipedia.org: RSA (cryptosystem)
[4] Ola Puchała

Załęcze Wielkie;
29.08.2024