Atakowanie RSA

Maciej Korpalski

7 grudnia 2018

RSA, przypomnienie schematu

- Klucz publiczny: N, e
- Klucz prywatny: N, d
- e i d spełniają: $d \cdot e = 1 (mod\ \phi(N))$
  gdzie ϕ - funkcja Eulera
- Wiadomość: m
- Szyfrowanie: $c = m^e (mod\ N)$
- Deszyfrowanie: $c^d = (m^e)^d = m\ (mod\ N)$

Faktoryzacja

Bezpieczeństwo RSA opiera się na trudności rozłożenia N na czynniki pierwsze.
Jeśli N $= p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$
to $\phi(N) = (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1}...(p_n - 1)p_n^{\alpha_n - 1}$
Znając $\phi(N)$ można łatwo wyliczyć d odwracając e modulo $\phi(N)$ (np. za pomocą rozszerzonego algorytmu Euklidesa).
Dlatego najbezpieczniej jest użyć $N = p \cdot q$ dla p, q - dużych liczb pierwszych.

Ataki na faktoryzację

W praktyce zadaniowej jeśli N ma mniej niż 150 cyfr, powinno się udać sfaktoryzowanie jej.
W tym celu polecam narzędzie yafu:
https://sourceforge.net/projects/yafu/
Jeśli podane jest kilka wartości N, można też sprawdzić, czy są względnie pierwsze.

Faktoryzacja Fermata

Ta metoda działa, jeśli p i q są podobnej wielkości, bliskiej do $\sqrt{N}$
Dla $N = p \cdot q$ można zauważyć, że $N = (\frac{(p+q)}{2})^2 - (\frac{(p-q)}{2})^2$
Czyli jeśli znajdziemy takie a, b, że $a^2 - N = b^2$
Wtedy p = a + b, q = a - b
W takim razie można sprawdzać kolejne wartości $\sqrt{N}$, $\sqrt{N} + 1$, $\sqrt{N} + 2$, ... Jeśli któraś z tych liczb jest kwadratem - można sfaktoryzować N

Niski wykładnik publiczny

Jeśli e jest małe (najczęściej 3), to dla krótkiej wiadomości szyfrogram może być mniejszy od N albo może być tylko kilka razy większy od N (przed nałożeniem modulo N). Wtedy wzięcie pierwiastka stopnia e zwróci oryginalną wiadomość.
Jeśli mamy dane e szyfrogramów tej samej wiadomości przy różnych N, można zastosować chińskie twierdzenie o resztach i potem pierwiastek stopnia e.

Niski wykładnik prywatny - atak Wienera

Niskie d można podejrzewać przy bardzo dużym e
Jeśli $d < \frac{1}{3}N^{\frac{1}{4}}$, to można skutecznie przeprowadzić następujący atak:
$e \cdot d = 1 \ (mod \ \phi(N))$
$e \cdot d = 1 + k \cdot \phi(N)$
$\frac{e}{\phi(N)} - \frac{k}{d} = \frac{1}{\phi(N)}$
$\phi(N)$ jest bardzo bliskie N, czyli $\frac{e}{N}$ jest bliskie $\frac{k}{d}$
Stosując przybliżenia przez ułamki łańcuchowe uda się znaleźć parę k, d spełniające warunki

Modyfikacja szyfrogramu

Dla danego szyfrogramu c można go zmodyfikować zmieniając w kontrolowany sposób zdeszyfrowaną wiadomość, której odpowiada
Dla stałej a $(a^e \cdot c)^d = a \cdot m \ (modulo\ N)$
Podobnie $(c^a)^e = m^a \ (modulo\ N)$

Bit Oracle

Jeśli znajdziemy funkcję znajdującą np. najmniejszy wiadomości jawnej na bazie szyfrogramu, to można ją odzyskać binsearchem
Po odzyskaniu pierwszego bitu mnożymy wiadomość przez 2^e, odzyskujemy ostatni bit nowej wiadomości.
Niezależnie od m, $2 \cdot m$ jest parzyste. N zazwyczaj jest nieparzyste, więc jeśli $m < \frac{N}{2}$, to otrzymamy 1, a 0 w przeciwnym przypadku.
Działając dalej w analogiczny sposób możemy odzyskać całą wiadomość

Sygnatury RSA i ich podrabianie

Sygnatura dla wiadomości m to m^d. Daje to możliwość sprawdzenia tożsamości osoby wysyłającej wiadomość, wystarczy do tego znajomość klucza publicznego
$(m^d)^e = m \ (mod \ N)$
Takie sygnatury można jednak bardzo łatwo podrobić - mając dane dowolne dwie sygnatury m_1^d, m_2^d można wygenerować kolejne, ponieważ $(m_1 \cdot m_2)^d$ też jest legalną sygnaturą (dla wiadomości $m_1 \cdot m_2$)

Ataki z dodatkowymi informacjami

Jeśli uda się znaleźć liczby A i B takie, że $A \cdot B = 0$ $(modulo\ N)$ oraz $A \neq B$, $1 < A, B < N$
To NWD(A, N) jest szukanym dzielnikiem N
W wielu zadaniach mamy jakieś dodatkowe dane, które pozwalają na znalezienie takich liczb i faktoryzację N