11. Kryptoanaliza systemu Rivesta – Shamira – Allemana (RSA)

Oznaczenia:

N =p*q (p, q – duże liczby pierwsze)
e – wukładanik szyfrujący
d – wykładnik deszyfrujący (prywatny) e*d=1 mod (p-1)(q-1)
E: $Z_n \longrightarrow Z_n$ – funkcja szyfrująca $E(m)=m^e(\text{mod } n)$
D: $Z_n \longrightarrow Z_n$ _ funkcja deszyfrująca $D(m) = m^d(\text{mod } n)$
S: $Z_n \longrightarrow Z_n$ – funkcja podpisu $S(m)=m^d(\text{mod } n)$
V: $Z_n \longrightarrow Z_n$ – funkcja weryfikacji podpisu $V(m)=m^e(\text{mod } n)$

Funkcja nadmiarowości:
Dla bezpieczeństwa systemu RSA wprowadzamy funkcję nadmiarowości h: $Z_n \longrightarrow Z_n$, która powoduje dołączenie dodatkowych bitów do wiadomości.
Powody tego są następujące:

1. Arytmetyczny charakter funkcji RSA (pozwala bo w szczególności na podpisanie dowolnej wiadomości zależnej multiplikatywnie od już podpisanych wiadomości bez znajomości klucza prywatnego) np. m_1 i m_2 $S(m_1)=m_1^d(\text{mod } n)=S(m_2)=m_2^d(\text{mod } n)$ $S(m_1,m_2)=(m_1m_2)^d=S(m_1)*S(m_2)(\text{mod } n)$
2. Bezpieczeństwo smeantyczne – szyfrogram może mieć pewne informacje na temat wiadomości np. funkcja RSA zachowuje symbol JACOBIEGO $\left(\frac{m}{N}\right)$ tzn. $\left(\frac{m}{N}\right)=\left(\frac{RSA[m]}{N}\right)$. Załóżmy, że $\left(\frac{m}{N}\right)=1$ i wtedy $RSA(m)=m^d$ więc $\left(\frac{RSA(m)}{N}\right)=\left(\frac{m^d}{N}\right)=\left(\frac{m}{N}\right)^d=1=\left(\frac{m}{N}\right)$ na mocy multiplikatywności symbolu JACOBIEGO oraz faktu, że wartości J są z {-1,0,1} oraz d jest nieparzyste.
3. Determinizm – jeśli szyfrogram jest funkcją zależną jedynie od oryginalnej wiadomości to podsłuchujący może łatwo ustalić, czy dwa kryptogramy pochodzą od tej samej wiadomości. Dla uniknięcia takiej sytuacji stosujemy zrandomizowaną funkcję nadmiarowości (lub znacznik czasowy)

System RSA zmodyfikowany funkcją nadmiarowości:
$E(m)=h(m)^e(\text{mod } n)$ $D(m)=h^{-1}(m^d) \text{ mod } n$ $h(m)=m||b_1||\_||b_k$ $b_i \in \{0,1\}$
$S(m)=h(m)^d(\text{mod } n)$ $V(m)= h^{-1}(m^e) \text{ mod } n$

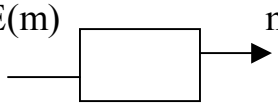
Rodzaje ataków:

1. Klasyfikacja według “siły” ataku
    - Tajność złamana – poznanie klucza prywatnego
    - Całkowita dedukcja – szyfrogram zdeszyfrowany bez znajomości klucza prywatnego
    - Częściowa dedukcja – jw. ale tylko dla pewnego podzbioru wiadomości (uprzednio nieznanych)
    - Częściowa informacja – możliwość uzyskania nietrywialnej informacji na temat wiadomości z jej kryptogramu

2. Klasyfikacja ze względu na założenia (typ ataku)
    - Atak pasywny – znany jest jedynie kryptogram wiadomości
    - Atak ze znanym tekstem jawnym – dysponujemy pewnym zbiorem kryptogramów i odpowiadającym im wiadomości.
    - Nieadaptywny atak z wybranym szyfrogramem – dysponujemy dostępem do „wyroczni” deszyfrującej, co pozwala na zdeszyfrowanie wybranych przez nas kryptogramów
    - Adaptywny atak z wybranym szyfrogramem – mamy dostęp do „wyroczni” w chwili przeprowadzania ataku, deszyfrujemy p[pewien kryptogram o który pytaliśmy wyroczni.

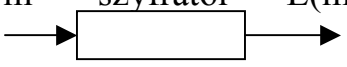
<u>Uwaga:</u> Analogicznie identyfikacja typów siły ataku mamy dla podpisu cyfrowego.

Przykład: nieadaptatywnego ataku z wybranym szyfrogramem

1. E(m)  m

    szyfrujemy kluczem publicznym właściciela karty

2. dostęp do urządzenia szyfrującego np. niezabezpieczonego komputera

    m szyfrator E(m)
    

Ataki na RSA:

1. Atak CoperSwitha – przy małym kluczu RSA i małych wiadomościach
2. Atak Hastada – stosowany np. gdy wiadomość jest wysyłana do różnych adresatów (lub jej kopia)
3. Ataki wykorzystujące powiązane wiadomości – 2 podobne wiadomości z podpisami

Ad 1.
m^e(mod n) dla e=3 (np.)
wtedy deszyfrogram jest pierwiastkowany w Z (ale nie w Z_n) i stosujemy algorytm przeszukiwania binarnego

Ad 2.
Zakładamy, że k>e k-liczba adresatów. Ten sam klucz publiczny dla różnych modułów RSA na mocy chińskiego twierdzenia o resztach obliczamy m^e(mod $N_1,...,N_k$) i pierwiastkujemy w Z

Ad 3.
$m_1=f(m_2)$ f-wielomian małego stopnia
Znajdujemy $e_1=m_1^e$ i m_2^e (mod n)
m_2 jest wspólnym pierwiastkiem wielomianu $g_2(x)=x^e-c_2$(mod n)
$g_1(x)=f(x)^e-c_1$(mod n)
zatem obliczając NWD($g_1(x)$, $g_2(x)$) znajdujemy czynnik liniowy x-c i wtedy $m_2-c=0$(mod n) => $m_2=c$(mod n) czyli poznajemy wiadomość m_2