Przemysław Zdrzalik *224466*
Dominik Kacprzak
Grzegorz Muszyński

Rok akademicki *2019/20*
Poniedziałek, 12:30

Podstawy Kryptografii – LABORATORIUM
Zadanie 3 – *Implementacja algorytmu DSA*

Opis rozwiązania

1. Generacja Parametrów

1.1. Należy wybrać funkcję produkującą ciąg **H** bitów. W przypadku naszego programu jest to SHA-1.
1.2. Należy wybrać długość klucza **L,** od 512 do 1024 bitów, oraz liczba bitów musi być podzielna przez 64.
1.3. Należy wybrać długość **N, N < L** oraz **N ≤ H**. W naszym przypadku długość N = 160 czyli taka sama jak długość outputu funkcji SHA-1
1.4. Należy wybrać taką liczbę pierwszą **q,** aby liczba jej bitów była równa **N.** W naszym przypadku jest to wykonane przez losowanie liczby o liczbie bitów **N**, tak długo aż okaże się ona liczbą pierwszą.
1.5. Należy wybrać taką liczbę pierwszą **p,** aby liczba jej bitów była równa **N,** oraz aby liczba **p-1** posiadała dzielnik **q**. W naszym przypadku jest to osiągnięte poprzez wymnażanie liczby **q** przez losową liczbę o liczbie bitów równej **L – N** oraz dodawanie do wyniku 1 aż otrzymamy liczbę pierwszą.
1.6. Należy wybrać losową liczbę całkowitą **h** z przedziału <2, **p**-2**>.**
1.7. Należy wyliczyć $\mathbf{g:=h^{(p-1)/q}}$ mod **p**
Otrzymane **p, q, g** są parametrami algorytmu.

2. Generacja Klucza publicznego i prywatnego

2.1. Należy wybrać losową liczbę całkowitą **x** z przedziału <1, **q**-1>.
2.2. Należy obliczyć $\mathbf{y = g^x}$ mod **p**
Otrzymane **x** i **y** są odpowiednio kluczem prywatnym i kluczem publicznym

3. Tworzenie Podpisu

3.1. Należy wybrać losową liczbę całkowitą **k** z przedziału <1, **q**-1>.
3.2. Należy obliczyć $\mathbf{r:=(g^k \bmod p) \bmod q}$
3.2. Należy obliczyć $\mathbf{s:=(k^{-1}(H(m) + xr)) \bmod q}$, gdzie **H(m)** jest wartością zwracaną przez wybraną funkcję hashującą przy obliczaniu wartości z wiadomości, dla której podpis chcemy utworzyć.
Podpisem jest para liczb (**r, s**)

4. Weryfikacja podpisu

4.1. Należy sprawdzić, czy 0 < **r** < **q** oraz 0 < **s < q**
4.2. Należy policzyć $\mathbf{w}:= \mathbf{s^{-1}}$ mod **q**
4.3. Należy policzyć $\mathbf{u_1}$:= **H(m) * w** mod **q**
4.4. Należy policzyć $\mathbf{u_2}$:= **r * w** mod **q**
4.5. Należy policzyć **v**:= $(\mathbf{g^{u1}y^{u2}}$ mod **p)** mod **q**
Jeżeli **v = r** to podpis jest właściwy

Źródła:

- https://en.wikipedia.org/wiki/Miller%E2%80%93Rabin_primality_test
- https://www.geeksforgeeks.org/multiplicative-inverse-under-modulo-m/
- https://en.wikipedia.org/wiki/Digital_Signature_Algorithm
- http://www.herongyang.com/Cryptography/DSA-Introduction-What-Is-DSA-Digital-Signature-Algorithm.html