Ziaur Rahman , 124606 <zia@iut-dhaka.edu>

Digital Signature Algorithm (DSA)

1 message

Rahman Ziaur <rahman.ziaur@rmit.edu.au> Tue, Mar 3, 2020 at 4:05 PM
To: zia <zia@iut-dhaka.edu>

Example 1 for Digital Signature Algorithm (DSA): DSA is a United States Federal Government standard for digital signatures and was proposed by NIST.

STEP 1: *Key generation*

- Choose a prime number **q**, which is called the prime divisor. Suppose q = 3
- Choose another primer number p, such that p-1 mod q = 0. p is called the prime modulus. p = 7 *[Choose an N-bit prime q. [Choose an L-bit prime p such that p − 1 is a multiple of q]*
- Choose an integer randomly from and Compute as if g is not equal to 2. Say h=2 , Therefore, g= h^(7-1)/2 = 2^2 = 4. The algorithm parameters are (, ,). These may be shared between different users of the system.
- Choose an integer, such that 0 < x < q. Choose an integer randomly from . Compute . Let's pick x=5. So, y = 4^5 mod 7 = 1024 mod = 2.
- Package the public key as {p,q,g,y}= {7, 3, 4, 2}.
- Package the private key as {p,q,g,x}= {7,3, 4, 5}.

STEP 2: *Signature generation* using private keys {p,q,g,x}= {7,3, 4, 5}..

- Generate the message digest h, using a hash algorithm like SHA1. Let's say Hash value of a message digest H(m) = 3
- Choose an integer randomly from . ∴, pick k = 2.
- Compute . In the unlikely case that r=0, start again with a different random . ∴ r = (4^2 mod 7) mod 3 = 2 mod 3 = 2.
- Compute . In the unlikely case that , start again with a different random . ∴ s = {2^{-1}(3 + 5x2)} mod 3 = 2(3+10) mod 3 = 26 mod 3 = 2.
- Package the digital signature as {r,s} = {2,2}.

STEP 3: *Verification*: using the public key {p,q,g,y}= {7, 3, 4, 2}.

- One can verify that a signature = (2,2) is a valid signature for a message as follows:

- Generate the message digest h, using the same hash algorithm. Suppose we are given the same message, so it will produce the same digest, H(m) = 3.

- Compute . ∴ $w = 2^{-1} \bmod 3 = 2$

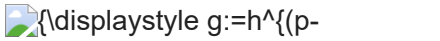

- Compute . ∴ $u_1 = 3 \times 2 \bmod 3 = 0$ and Compute . ∴ $u_2 = 2 \times 2 \bmod 3 = 1$.

- Compute . ∴ $v = (4^0 \times 2^1 \bmod 7) \bmod 3 = (1 \times 2 \bmod 7) \bmod 3 =$  2 and the signature is valid if and only if .

Pseudocode:

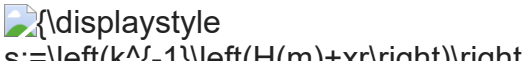
Example 2:

Key Gen:

- Let a Prime divisor, q = 11 and it should multiple of (p-1), lets calculate p = 2 x q + 1 = 23.
- Pick integer randomly from and Compute  . h should within 2 to 21, Let's take h = 2, ∴ $g = 2^{22/11} \bmod 23 = 4$.
- Take an integer randomly from . Compute  . Let's pick x=7. So, y = 4^7 mod 23 = 16384 mod 23 = 8.
- ∴ public key as {p,q,g,y}= {23, 11, 4, 8}.
- ∴ private key as {p,q,g,x}= {23,11, 4, 7}.

Sign:

- Let's say Hash value of a message digest H(m) = 3. pick k = 5.
- . ∴ $r = (4^5 \bmod 23) \bmod 11 = 12 \bmod 11 = 1$.



- . ∴ $s = \{5^{-1}(3 + 7x1)\} \bmod 11 = 9(3+7) \bmod 11 = 90 \bmod 11 = 2$.
- Package the digital signature as {r,s} = {1,2}.

Verify:

- ∴ **H(m) = 3 and given signature (r,s) = (1,2)**

- . ∴ $w = 2^{-1} \bmod 11 = 6$


- . ∴ u_1= 3 x 6 mod 11 = 7 and Compute

. ∴ u_2= 1x6 mod 11 = 6.

- . ∴ v = (4^7 x 8^6 mod 23) mod 11 = (16384 x 262144 mod 23) mod 11 = (8 x 13 mod 23) mod 11 = (104 mod 23) mod 11 = 12 mod 11 = 1 and the signature is valid.
