Ehren Schindelar
RIN 661677600
Oct. 14, 2018

1

a) A's public key is $\alpha^{X_A} \mod q = 7^5 \mod 71 = 51$

b) B's public key is $\alpha^{X_B} \mod q = 7^12 \mod 71 = 4$

c) The shared secret key is $Y_A^{X_B} \mod q = Y_B^{X_A} \mod q = 4^5 \mod 71 = 30$

d) The particiapants may not end up with the same private key. The Diffie-Hellman key exchange protocol relys on the fact that $(x^a)^b \mod p = (x^b)^a \mod p$. If instead of taking an agreed upon value to the power of some secret, and took a secret value to the power of an agreed upon value, they would run into the problem that $b^{(a^x)} \mod p$ is not neccesarily equal to $a^{(b^x)} \mod p$.

Ehren Schindelar
RIN 661677600
Oct. 14, 2018

2

a) An attacker can perform a Birthday Attack on the network to get them to sign something they didn't want to. This can be done by finding two different messages with the same hash function value, since the resource's signature is based only on that hash value. This is done by slightly altering either message until a matching pair is found. The attacker can then send one version to the network for it to sign, and append that signature to the other version.

b) An attacker would need $64^2 * M$ bits of memory in the worst possible case.

c) $n(p; H) \approx \sqrt{2Hln(1/(1-p))}$
$n(.5; 2^{64}) \approx \sqrt{2^{65}ln2}$
$n(0.5; 2^{64}) \approx 5056937541$
Which at 2^{20} hash/second would take about 4800 seconds, or 1 and 1/3 hours

d) With a 128-bit hash, you would need $128^2 * M$ bits of memory, and on average would take 2^{13} seconds, more than 650,000 years, to find a collision.

Ehren Schindelar
RIN 661677600
Oct. 14, 2018

3

Plaintext $P = (01010111)$

Private key: $S = (5, 8, 21, 45, 103, 215, 450, 946)$

multiplier: $a = 1019$, and modulus: $p = 1999$

Step 1: compute public key A

$A_i = S_i * a \mod p$

$A = (1097, 156, 1409, 1877, 1009, 1194, 779, 456)$

Step 2: compute ciphertext C

$C = \sum_i^n A_i * P_i$

$C = 156 + 1877 + 1194 + 779 + 456$

$C = 4462$

Step 3: decrypt ciphertext to plaintext P_2

Find the modular multiplicative inverse of $a \mod p$ using the extended euclidian algorithm

$$\begin{gathered}
1999 = 1019 + 980 \\
1019 = 980 + 39 \\
980 = 25 * 39 + 5 \\
39 = 7 * 5 + 4 \\
7 = 4 + 3 \\
4 = 3 + 1 \\
980 = 1999 - 1019 \\
39 = 1019 - 980 = 2 * 1019 - 1999 \\
5 = 980 - 25 * 39 = 26 * 1999 - 51 * 1019 \\
3 = 39 - 7 * 5 = 359 * 1019 - 183 * 1999 \\
1 = 4 - 3 = 209 * 1999 - 410 * 1019 \\
a^{-1} \mod p = -410
\end{gathered}$$

$C' = C * a^{-1} \mod p$

$C' = 1664$

We can solve the subset sum easily using the private key since S is superincreasing

$C' = 946 + 450 + 215 + 45 + 8$

$P_2 = (0, 1, 0, 1, 0, 1, 1, 1)$