9

Homework 5 Cryptography

Rick Staals 0716184
Erwin van Duijnhoven 0719562

October 9, 2013

Exercise 1

0/2

The integer $p = 1009$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 123$. You observe $h_a = 234$ and $h_b = 456$. What is the shared key of Alice and Bob?

Answer

We know that $n_a \cdot g = h_a$ & $n_b \cdot g = h_b$.
We will first compute $n_a = g^{-1}h_a \bmod (1009)$.
For this we will need the inverse of g such that $g \cdot g^{-1} = 1 \bmod (1009)$.
If we know the order δ of g then we know that $g^{\delta-1} = g^{-1}$

$$\begin{array}{rcrcrcll}
g^2 & \equiv & 123^2 & \equiv & 15129 & \equiv & 1003 & \mathrm{mod}(1009) \\
g^4 & \equiv & 1003^2 & \equiv & 1006009 & \equiv & 36 & \mathrm{mod}(1009) \\
g^8 & \equiv & 36^2 & \equiv & 1296 & \equiv & 287 & \mathrm{mod}(1009) \\
g^{16} & \equiv & 287^2 & \equiv & 82369 & \equiv & 640 & \mathrm{mod}(1009) \\
g^{32} & \equiv & 640^2 & \equiv & 409600 & \equiv & 955 & \mathrm{mod}(1009) \\
g^{64} & \equiv & 955^2 & \equiv & 912025 & \equiv & 898 & \mathrm{mod}(1009) \\
g^{128} & \equiv & 898^2 & \equiv & 806404 & \equiv & 213 & \mathrm{mod}(1009) \\
g^{256} & \equiv & 213^2 & \equiv & 45369 & \equiv & 973 & \mathrm{mod}(1009) \\
g^{512} & \equiv & 973^2 & \equiv & 946729 & \equiv & 287 & \mathrm{mod}(1009)
\end{array}$$

We see that $g^8 = g^{512}$ which means the order of g ~~is at most~~ divides 504. Therefore $g^{503} = g^{-1}$.

$$\begin{gathered}
g^{503} \equiv \\
g^{256+128+64+32+16+4+2+1} \equiv \\
973 \times 213 \times 898 \times 955 \times 640 \times 36 \times 1003 \times 123 \equiv \\
505.196.893.258.601.241.600 \equiv \\
484 \ \mathrm{mod}(1009)
\end{gathered}$$

true, but complicated way of finding an inverse
use xgcd instead

$$\begin{array}{rcrcrl}
n_a & \equiv & 234 \times 484 & \equiv & 248 & \mathrm{mod}(1009) \\
n_b & \equiv & 456 \times 484 & \equiv & 742 & \mathrm{mod}(1009) \\
g \cdot n_a \cdot n_b & \equiv & 123 \times 248 \times 742 & \equiv & 80 & \mathrm{mod}(1009)
\end{array}$$

So the shared key of Alice and Bob is 80.

4/4

Exercise 2

Alice and Bob use the DH key exchange in $\mathbb{F}_{2^4} \cong \mathbb{F}_2[x]/(x^4+x+1)$ with $g = x$. Find the order of g. Alice uses $n_A = 4$, Bob uses $n_B = 7$. Compute all parts of the key exchange, i.e. h_A,h_B and the shared key.

Answer

The number of elements $|\mathbb{F}_{2^4}| = 15 = 3 \times 5$ so the subgroups have an order of $\{1, 3, 5, 15\}$

$$
\begin{aligned}
x^1 &\equiv & & x^1 & &\mod(x^4+x+1) \\
x^3 &\equiv & & x^3 & &\mod(x^4+x+1) \\
x^5 &\equiv & & x^2+x & &\mod(x^4+x+1) \\
x^{15} &\equiv (x^2+x)^3 & &\equiv x^6+x^5+x^4+x^3 & & \\
&\equiv (x^3+x^2)+(x^2+x)+(x+1)+(x^3) & &\equiv 1 & &\mod(x^4+x+1)
\end{aligned}
$$

g has an order 15.

$$
\begin{aligned}
x^{n_A} &\equiv & x^4 &\equiv & x+1 & &\mod(x^4+x+1) \\
x^{n_B} &\equiv & x^7 &\equiv & x^3+x+1 & &\mod(x^4+x+1) \\
x^{n_A \cdot n_B} &\equiv & x^{28} \equiv x^{13} &\equiv & x^7x^6 & & \\
&\equiv & (x^3+x+1)(x^3+x^2) &\equiv & x^6+x^5+x^4+x^2 & & \\
&\equiv & (x^3+x^2)+(x^2+x)+(x+1)+x^2 &\equiv & x^3+x^2+1 & &\mod(x^4+x+1)
\end{aligned}
$$

so $h_A = x+1$, $h_B = x^3+x+1$ and the shared key is x^3+x^2+1.

Exercise 3

Here is a public key system.
Key set up. Each user does the following

- Choose any two integers a and b.
- Set $M = ab - 1$.
- Choose two more integers a' and b'.
- Set $e = a'M + a$ & $d = b'M + b$, and $n = (ed - 1)/M$.

The public key is (n, e), the secret key is d. Encryption: To encrypt a plaintext message m to public key (n, e) compute

$$c \equiv em \bmod n.$$

The owner of d can decrypt this by computing

$$m' \equiv dc \bmod n.$$

1. Set up your secret key and private key starting from $a = 100$, $b = 103$, $a' = 39$, $b' = 51$. Decrypt $c = 42$.
2. Why is n an integer? Why does the system work, i.e. why is $m' = m$? Show how to obtain the secret key corresponding to the target pubic key $(118, 857)$.

Answer 1

1/1

With given values it follows that $M = 10299$, $e = 401761$, $d = 525352$ & $n = 20493829$.

Then

$$m' \equiv dc \equiv 22064784 \equiv 1570955 \bmod 20493829$$

Answer 2

We first show that n is an integer.

$$\begin{aligned} n &= \frac{ed - 1}{M} \\ &= \frac{(a'M + a)(b'M + b) - 1}{M} \\ &= \frac{a'b'M^2 + ab'M + a'bM + ab - 1}{M} \\ &= \frac{a'b'M^2 + ab'M + a'bM + M}{M} \\ &= a'b'M + ab' + a'b + 1 \end{aligned}$$

3/3

This clearly is an integer.

Now we show that $m' = m$. We suppose that $m < n$. We see that $Mn = ed - 1$, so $ed \equiv 1 \mod n$. This clearly means

$$\begin{aligned} m' &\equiv dem \mod n \\ &\equiv m \mod n. \end{aligned}$$

This means that $m = m'$

We try to obtain the secret key d when $(n, e) = (118, 857)$. For this, we see that $ed \equiv 1 \mod n$. This means that (if $e^{-1} \mod n$ exists) $d = e^{-1} + 118k$, with k an integer. We calculate $e^{-1} \mod n$ by using the extended Euclidean algorithm on 118 and $31 (\equiv 857 \mod 118)$.

Step	a	b
0	[118,1,0]	[31,0,1]
1	[31,0,1]	[25,1,-3]
2	[25,1,-3]	[6,-1,4]
3	[6,-1,4]	[1,5,-19]
4	[1,5,-19]	[0,-31,118]

So this means that $1 = 5 \cdot 118 - 19 \cdot 31$, so $-19 \cdot 31 \mod 118 \equiv 1 \mod n$, so $31^{-1} \mod n \equiv -19 \mod 118 \equiv 99 \mod 118$. Therefore $d = 99 + 118k$ with k an integer. For future calculations in the decryption, taking $d = 99$ is sufficient, because $m' \equiv (99 + 118k)c \mod n \equiv 99c \mod n$.