EXERCISES 5 TMA4160 - KRYPTOGRAFI

Ch. 6

2. Let $a = \log_\alpha(\beta)$ with $a \in [s,t]$ for $0 \leq s < t < n$ where n is the order of α in the group G. By setting $n = t - s$ in SHANKS(G, n, α, β) we get an algorithm with complexity $O(\sqrt{t-s})$. The proof of this is exactly the same as in the book, with n substituted.

3. Set $p = 458009$ and $\alpha = 2$. Then p is a prime and α has order $n = 57251$ in $\mathbb{Z}_p^*$. We use Pollard-rho to compute the discrete logarithm of $\beta = 56851$ to the base α in $\mathbb{Z}_p^*$. Set $x_0 = 1$ and define (S_1, S_2, S_3) by:

$$S_1 = \{x \in \mathbb{Z}_p : x \equiv 1 \mod 3\}$$
$$S_2 = \{x \in \mathbb{Z}_p : x \equiv 0 \mod 3\}$$
$$S_3 = \{x \in \mathbb{Z}_p : x \equiv 2 \mod 3\}$$

$x_0 = 1$ implies that $a_0 = b_0 = 0$, so by following the algorithm we get a collision when $i = 444$ yielding:

$$(x_i, a_i, b_i) = (339768, 22811, 35067)$$
$$(x_{2i}, a_{2i}, b_{2i}) = (339768, 37251, 5360)$$

So when solving $c(b_{2i} - b_i) = (a_i - a_{2i}) \mod n$ we get that $c \equiv 40007 \mod n$ and so $2^{40007} \equiv 56851 \mod p$, or $\log_2(56851) = 40007$.

5. Let p be a prime and α a primitive element. The following is a Matlab code for the Pohlig-Hellman algorithm:

```
function [ Dlog ] = PohligHellman( alpha, beta, n )
%Solves alpha^a = beta mod n for a.

%find factors
C = TrialDiv(totient(n));
r = length(C);

%compute the sublogproblem
a=zeros(1,r);
for i=1:r
    q=C(1,i);
    j=0;
    Beta = zeros(1,C(2,i));
    aj=zeros(1,C(2,i));
    Beta(1) = beta;
    a(i)=0;
    while j <= C(2,i)-1
        delta = modexp(Beta(1,j+1),totient(n)/(q^(j+1)),n);
        for k=0:q-1
            gamma=modexp(alpha, (k*totient(n))/q,n);
            if gamma==delta
                aj(1,j+1)=k;
                break
            end
        end
        ainv=lincon(alpha,1,n);
        Beta(1,j+2) = mod(Beta(1,j+1).*modexp(ainv(1,1),(aj(1,j+1)*q^j),n),n);
        a(1,i) = mod(a(1,i) + aj(1,j+1)*q^j,q^C(2,i));
        j=j+1;
    end
end
%C.R.T.
M=C(1,:).^(C(2,:));
Dlog = lincon(1,a,M);
end
```

Where the lincon function is a function solving linear congruences and TrialDiv is a trial division function for finding the prime factors. Note that this assumes that n is "sufficiently small". Using this we calculate $\log_5(8563) \in \mathbb{Z}_{28703}$ and $\log_{10}(12611) \in \mathbb{Z}_{31153}$ to be 3909 and 17102 respectively.

6. Let $p = 227$. Then $\alpha = 2$ is primitive in $\mathbb{Z}_p^*$.

a) We calculate modulo p:

$$2^{32} = 176 = 2^4 \cdot 11$$
$$2^{40} = 110 = 2 \cdot 5 \cdot 11$$
$$2^{59} = 60 = 2^2 \cdot 3 \cdot 5$$
$$2^{156} = 28 = 2^2 \cdot 7$$

b) Let log be the discrete logarithm with base 2 in $\mathbb{Z}_p^*$. Then $\log(2) = 1$. From the previous exercise we then have (modulo $p-1$):

$$28 \equiv \log(11)$$
$$39 \equiv \log(5) + \log(11)$$
$$57 \equiv \log(3) + \log(5)$$
$$154 \equiv \log(7)$$

This yields: $\log(3) = 46, \log(5) = 11, \log(7) = 154, \log(11) = 28$.

c) We calculate $\log(173)$ by following the hint in the book; Multiply 173 by $2^{177} \mod p$. We then get $173 \cdot 2^{177} \equiv 168 \mod p$ which implies that $\log(173) + 177 \equiv \log(168) \mod p-1$. Now note that $168 = 2^3 \cdot 3 \cdot 7$ and so $\log(168) = 3 + 46 + 154 = 203$. We therefore have that $\log(173) = 26$.

10. Observe that a polynomial of degree 5 is irreducible if and only if it has no linear or quadratic factors. To check the linear factors note that if $f(x) = (x-a)q(x) + r(x)$ and $f(a) = 0$, then $r(x) = 0$ and so f is reducible. Therefore we cannot have $f(a) = 0$ for any $a \in \mathbb{Z}_2$ (since the division algorithm is true for polynomials!). This rules out the polynomial $f(x) = x^5 + x^4 + x^2 + 1$ as $f(1) = 0$. We now use the subtle fact that $x^2 + x + 1$ is the only irreducible polynomial of degree 2 and $x^3 + x^2 + 1, x^3 + x + 1$ is the only irreducible polynomials of degree 3 in $\mathbb{Z}_2[x]$. Since we have shown that the two other candidates have no linear factors, we can show that they are irreducible by showing that they have no quadratic or cubic factors either. Since we know the irreducible polynomials of those degrees we can multiply them to see that the only reducible polynomials degree of 5 (which haven't got a linear factor) is: $x^5 + x + 1$ and $x^5 + x^4 + x^2 + x + 1$. Therefore the two other polynomials must be irreducible.

11. $\mathbb{F}_{2^5} \simeq \mathbb{Z}_2[x]/(x^5 + x^2 + 1)$.

a) We compute $(x^4 + x^2) \times (x^3 + x + 1) = x^7 + 2x^5 + x^4 + x^3 + x^2$. Now since we operate in $\mathbb{Z}_2[x]/(x^5 + x^2 + 1)$ we can extract two things: $2x^5 = 0$ and $x^5 = -(x^2 + 1)$. This implies that $(x^4 + x^2) \times (x^3 + x + 1) = x^3$.

b)

c)