EXERCISES 4, TMA4160 - KRYPTOGRAFI

Ch. 6

4.

c) By a) we need to find an element α such that α is a primitive root modulo 29, but $\alpha^{p-1} \equiv 1 \mod 29^2$. By some trial and error we eventually find that 14 is the smallest integer such that it is a primitive root modulo 29, but not modulo 29^2 (Note that $14 + 29 = 43$ however is a primitive root in 29^2).

d) Set $n = 24389$, $\beta = 3344$ and $\alpha = 3$ with $\alpha^a = \beta$. We now compute $a = \log_\alpha(\beta) = \log_3(3344)$ in the group $\mathbb{Z}^*_{24389}$ using Pohlig-Hellman. We compute the order of the group and factor it to obtain $|\mathbb{Z}^*_n| = \phi(n) = 2^2 \cdot 7 \cdot 29^2$. We compute the linear congruences that constitute the solution via. the Chinese remainder theorem. First we set $q = 2$, $c = 2$ and $a = a_0 + 2a_1$. Using that $\beta^{\phi(n)/q} = \alpha^{a_0\phi(n)/q} \Rightarrow 3344^{11774} \equiv 24388^{a_0} \mod 24389 \Rightarrow 1 \equiv 24388^{a_0} \mod 24389$ implying that $a_0 = 0$. Now using the recurrence relation $\beta_{j+1} = \beta_j \alpha^{-a_j q^j}$ we get $\beta_1 = \beta$ and from $\beta_j^{n/q^{j+1}} = \alpha^{a_j n/q}$ we have $\beta^{\phi(n)/q^2} = \alpha^{a_0\phi(n)/q} \Rightarrow 3344^{5887} \equiv 24388^{a_1} \mod 24389$ implying that $a_1 = 1$. In other words we have $a \equiv 2 \mod 4$. Similarly we get $a \equiv 2 \mod 7$ and $a \equiv 260 \mod 29^2$. This gives:

$$\begin{aligned} a &\equiv 2 \mod 4 \\ a &\equiv 2 \mod 7 \\ a &\equiv 260 \mod 841 \end{aligned}$$

Solving this system by applying the Chinese remainder theorem we get that $\log_3(3344) = a \equiv 18762 \mod \phi(n)$.

Ch. 5

20. The MATLAB-code for this exercise is given below:

```
function [s] = JacSym(m,n)
%Jacobi symbol of (m/n), where n is always odd.

if mod(n,2)==0
    fprintf('Error: is not odd.\n');
end

m=mod(m,n);

if mod(n,2)==0
    s=0;
elseif m==1;
    s=1;

elseif mod(m,2)==0
    if abs(mod(n,8))==1
        s=JacSym(m/2,n);
    else
        s=-JacSym(m/2,n);
    end
else
    if mod(n,4)==3 && mod(m,4)==3
        s=-JacSym(n,m);
    else
        s=JacSym(n,m);
    end
end
end
```

This gives:

$$\left(\frac{610}{987}\right) = -1, \left(\frac{20964}{1987}\right) = 1, \left(\frac{1234567}{11111111}\right) = 1$$

21. We are given $n = 837, 851, 1189$ and we are asked to find the number of bases b such that n is an Euler pseudoprime to the base b; I.e. $\gcd(b, n) = 1$ and $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \mod n$. Using the function above in a simple for-loop checking for gcd we find that the number of bases are: 1, 1 and 7 respectively. We can also keep track over the numbers that are Euler pseudoprimes and get:

$$n = 837 \text{ gives the base: } 836$$
$$n = 851 \text{ gives the base: } 850$$
$$n = 1189 \text{ gives the bases: } 204, 278, 360, 829, 911, 985, 1188$$

(Note that we have excluded the case $b = 1$).

22. Define:

$$G(n) = \{a : a \in \mathbb{Z}_n^*, \left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \mod n\}$$

a) Obviously $G(n) \subset \mathbb{Z}_n^*$ and since $1 \in G(n)$ we need to show that it is also a group. That is, we need to show that if $a, b \in G(n)$, then $ab^{-1} \in G(n)$. Since $a, b \in G(n)$ and $G(n) \subset \mathbb{Z}_n^*$ we have that there is an $b^{-1} \in \mathbb{Z}_n^*$ such that $bb^{-1} = 1$. We therefore have:

$$1 = \left(\frac{1}{n}\right) = \left(\frac{b}{n}\right)\left(\frac{b^{-1}}{n}\right) \equiv b^{(n-1)/2}\left(\frac{b^{-1}}{n}\right) \Rightarrow \left(\frac{b^{-1}}{n}\right) = \left(b^{(n-1)/2}\right)^{-1} = \left(b^{-1}\right)^{(n-1)/2}$$

It now follows that

$$\left(\frac{ab^{-1}}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b^{-1}}{n}\right) \equiv (a)^{(n-1)/2}\left(b^{-1}\right)^{(n-1)/2} = \left(ab^{-1}\right)^{(n-1)/2}$$

And hence $G(n)$ is a subgroup of $\mathbb{Z}_n^*$. Assume the inclusion is proper; Set $|G(n)| = G$ and $|\mathbb{Z}_n^*| = P = \phi(n)$. Then by Lagrange's theorem we have $G|P \Leftrightarrow kG = P$ for some (positive) integer k. Since the inclusion is proper, and $G(n)$ is nonempty we have that the smallest such k is 2, i.e. $2G \leq kG = P$. This and the fact that $\phi(n) \leq n-1$ yields:

$$|G(n)| \leq \frac{|Z_n^*|}{2} \leq \frac{n-1}{2}$$

b) Now suppose that $n = p^k q$ where p and q are odd, p prime, $k \geq 2$ and $\gcd(p,q) = 1$. Let $a = 1 + p^{k-1}q$. Consider:

$$a^{(n-1)/2} = \left(1 + p^{k-1}q\right)^{(n-1)/2} = \sum_{i=0}^{(n-1)/2} \binom{(n-1)/2}{i} \left(p^{k-1}q\right)^i$$

Now since $M = \left(p^{k-1}q\right)^i = \left(p^{k-1}\right)^i q^i$ we see that M is a multiple of n for all $i \geq 2$. Therefore:

$$a^{(n-1)/2} \equiv 1 + \frac{(n-1)}{2}p^{k-1}q$$

Furthermore:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)^k \left(\frac{a}{q}\right) = 1$$

Due to the properties of the Jacobi symbol. Therefore for the property $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \mod n$ to hold we must have $\frac{(n-1)}{2}p^{k-1}q \equiv 0 \mod n \Leftrightarrow (p^k q)|\frac{(n-1)}{2}p^{k-1}q \Leftrightarrow p|\frac{(n-1)}{2} \Leftrightarrow n \equiv 1 \mod p$ which is impossible! Therefore we get:

$$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \mod n$$

c) Suppose $n = p_1 \cdots p_s$ where the factors are distinct primes greater than 2. Suppose $a \equiv u \mod p_1$ and $a \equiv 1 \mod p_2 p_3 \cdots p_s$ where u is a quadratic non-residue modulo p_1 (Use C.R.T. for this). Note that:

$$\left(\frac{a}{n}\right) = \left(\frac{u}{p_1}\right)\left(\frac{1}{p_2 \cdots p_s}\right) = -1$$

From the properties of the Jacobi symbol and the assumptions. Furthermore:

$$a^{(n-1)/2} \equiv 1^{(n-1)/2} = 1 \mod p_2 \cdots p_s$$

Now since $q|n$ we also have $a^{(n-1)/2} \equiv 1 \mod n$. And so $a^{(n-1)/2} \not\equiv -1 = \left(\frac{a}{n}\right) \mod n$.

d) Let n be odd and composite.

e)

Exercises.

c) The Matlab-code for the function is given below:

```
function [ S ] = MAC( A,k,l )
n=length(A);
A=double(A)-97;
S=1;
```

```
for i=1:n
    if A(1,i)==-65
        A(1,i)=28;
    elseif A(1,i)==-53
        A(1,i)=27;
    elseif A(1,i)==-51
        A(1,i)=26;
    end
    S=S+A(1,i)*modexp(k,i,456979);
    S=mod(S,456979);
end
S = mod(S + modexp(k,n+1,456979),456979);
end
```

d) Using the code above we see that the message that corresponds to the MAC 230887 is "invest in penny stocks".