December 17, 2013

Exam in TMA4160 Cryptography. Solution sketch.

Problem 1

(i) Easy computation.

(ii) We have been given two matrices A and B that are inverses modulo 26. The first matrix given corresponds to the letters `hell`, which means that the matrix C corresponding to the first four ciphertext letters satisfies $C = AK$. We get that $K = BC$, which gives us

$$K = \begin{pmatrix} 1 & 0 \\ 3 & 5 \end{pmatrix}.$$

The matrix K is easy to find an inverse of, and the decryption of the final four letters is found to be `obob`.

Note that the first `o` matches the final letter of the known plaintext, which is good.

Problem 2

(a) We use the function $f(x) = x^2 + 1$ and start with $s_0 = 14$ and $t_0 = f(s_0)$. We then compute the sequence $s_i = f(s_{i-1})$ and $t_i = f(f(t_{i-1}))$:

i	s_i	t_i	$\gcd(n, s_i - t_i)$
0	14	197	1
1	197	23411	53

We get that $n = 53 \cdot 541$.

(b) We can compute an inverse of 7 modulo $540 \cdot 52$, giving the decryption key $(n, 8023)$. But if we compute the inverse modolu $\operatorname{lcm}(540, 52) = 7029$, we get the decryption key $(n, 1003)$, which will speed up computations in the next problem slightly.

(c) We compute the following table

i	0	1	2	3	4	5	6	7	8	9
$2^{2^i} \bmod n$	2	4	16	256	8190	9953	25667	4041	14744	15523

Then we compute $1003 = 2^0 + 2^1 + 2^3 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9$ and

$$2^{1003} \equiv 2 \cdot 4 \cdot 256 \cdot 9953 \cdot 25667 \cdot 4041 \cdot 14744 \cdot 15523 \equiv 10084 \pmod{n}.$$

The total workload is 9 squarings and 7 multiplications.

Problem 3

(a) We find that $10 \equiv 1 \pmod 3$ and $6 \equiv 1 \pmod 5$, so $N \equiv 10 + 24 \equiv 4 \pmod{15}$.

Hasse's theorem says that $|N - p - 1| \leq 2\sqrt{p}$, which means that $82 \leq N \leq 122$. The numbers in that range that are congruent with four modulo 15 are 94, 109 and 124, and 109 is the only possible prime.

(b) There are many ways to approach this problem, but it makes sense to spend some time finding a short sequence of computations.

Keeping in mind that doublings are more expensive than additions, one fairly short sequence is to observe that we only need to show that $6P$ and $2Q + R$ are inverses, and that $2P$ and $Q + 2R$ are inverses. These can be computed as follows:

$2P$	$Q + R$
$4P = 2(2P)$	$2Q + R = Q + (Q + R)$
$6P = 2P + 4P$	$Q + 2R = (Q + R) + R$

The workload is 2 doublings and 4 additions. Ignoring additions and subtractions, each doubling costs 6 multiplications (or 5 if division by 2 is handled cleverly) and 1 inversion, while each addition costs 3 multiplications and 1 inversion. The total workload is dominated by the 24 multiplications and the 6 inversions.

(c) We solve the linear system and get $\log_P R = 37$.

Problem 4

We observe that 1 has Legendre symbol 1 and -1 has Legendre symbol -1 (since it $(p-1)/2$ is odd). Furthermore, we see that x is a square, so w is a square if and only if the ciphertext is an encryption of 1. Using the standard algorithm for computing Jacobi symbols, we compute that w has Legendre symbol -1.

Problem 5

(a) We solve the linear equation $2a \equiv -32 \pmod{53}$ and find that $\log_g y = 37$.

(b) We observe that the two values $g^3 y^{-50}$ and $g^{35} y^{-48}$ involved in the verification equation correspond to the equation given in (a). Which means that the signing key is 37 and, more important, the same random number was used to sign both messages! The random number can be found as

$$r \equiv w - av \equiv 8 \pmod{53}.$$