Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam:
Kristian Gjøsteen 73 55 02 42

EXAM IN TMA4160 CRYPTOGRAPHY

English
Saturday, December 18, 2010
Time: 0900-1300
Any printed or hand-written material is allowed during the exam.
An approved, simple calculator is allowed.

All problems have equal weight. Show your work.

Problem 1 Let $\mathbb{F}_{29}$ be the field with 29 elements, the elements represented by $0, 1, 2, \dots, 28$. Let $\mathcal{A} = \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \dots, \mathrm{Z}\}$ be the letters of the alphabet. We map $\mathcal{A}$ into $\mathbb{F}_{29}$ in the obvious way, A $\mapsto 0$, B $\mapsto 1$, …, Z $\mapsto 25$.

Strings of letters become strings of field elements in the obvious fashion. We map strings of field elements to polynomials in $\mathbb{F}_{29}[X]$ as follows:

$$(m_1, m_2, \dots, m_l) \longmapsto m_1 X + m_2 X^2 + \cdots + m_l X^l.$$

We have now defined how a string m of letters maps to a polynomial $m(X)$, e.g. CAR maps to the polynomial $2X + 0X^2 + 17X^3$.

Next, define the message authentication code

$$f(k_1, k_2, m) = m(k_1) + k_2,$$

where $k_1, k_2 \in \mathbb{F}_{29}$, m is a string of letters and $m(k_1)$ denotes the evaluation of the polynomial $m(X)$ in k_1.

a) You share the key $k_1 = 3$, $k_2 = 21$ with Alice. You receive two messages $(\mathrm{HELP}, 24)$ and $(\mathrm{OK}, 24)$, both claiming to be from Alice. Which message is from Alice?

b) You know that Carol shares a secret key with Bob. You intercept the two messages $(\text{KELP}, 7)$ and $(\text{HELP}, 21)$ from Carol before they reach Bob. Compute a field element t such that Bob will believe (OK, t) came from Carol.

Problem 2

a) Use the Soloway-Strassen algorithm with random choice 650 to decide if 1829 is prime or composite.

b) Use Pollard's ρ method with the polynomial $f(x) = x^2 + 1$ to factor 1829, using 2 as a starting point.

c) Use the following relations to factor 1829:

$$807^2 \equiv 5^3 \pmod{1829}$$
$$1656^2 \equiv 5 \cdot 7 \cdot 19 \pmod{1829}$$
$$1150^2 \equiv 7 \cdot 19 \pmod{1829}$$

Problem 3 Let p and q be primes such that $\gcd((p-1)(q-1), pq) = 1$. Set $n = pq$. The group $\mathbb{Z}_{n^i}^*$ has order $(p-1)(q-1)n^{i-1}$. Denote by $a + \langle n^i \rangle$ the equivalence class in $\mathbb{Z}_{n^i} = \mathbb{Z}/\langle n^i \rangle$ containing a.

a) Let $g = 1 + n + \langle n^2 \rangle \in \mathbb{Z}_{n^2}^*$. Prove that for any non-negative integer m,

$$g^m = 1 + mn + \langle n^2 \rangle,$$

and that g has order n.

Hint: $(a+b)^c = \sum_{i=0}^{c} \binom{c}{i} a^i b^{c-i}$.

Let $H = \{x^n \mid x \in \mathbb{Z}_{n^2}^*\}$. Let $\phi : \mathbb{Z}_n^* \to \mathbb{Z}_{n^2}^*$ be the map given by

$$a + \langle n \rangle \mapsto a^n + \langle n^2 \rangle.$$

b) Prove that H is a subgroup of $\mathbb{Z}_{n^2}^*$ and that H is the image of ϕ.

c) Prove that ϕ is a group isomorphism from $\mathbb{Z}_n^*$ to H.

Let u be any inverse of n modulo $(p-1)(q-1)$.

d) Prove that for any $x \in H$ and $m \in \mathbb{Z}$,

$$(xg^m)^{un} = x.$$

We can define a public key cryptosystem as follows:

- Key generation is to find an RSA modulus as above. The encryption key is n, the decryption key is (n, u).
- We encrypt $m \in \{0, 1, \ldots, n-1\}$ by choosing a random element $r \in \mathbb{Z}_n^*$, then computing the ciphertext as

$$c = \phi(r)g^m.$$

e) Explain how to decrypt ciphertexts using u and n.