Norwegian University of Science and Technology
Department of Mathematical Sciences

Contact during the exam:
George Petrides (735)91695

EXAM IN TMA4160 CRYPTOGRAPHY

English
Monday, December 12, 2011
Time: 09.00–13.00
Any printed or hand-written material and an approved simple calculator are allowed.
Solve all four (4) problems. Show all your work and justify all answers.

Problem 1 Alice invites Bob to resolve their "who will do the dishes" dispute over coin-flipping as follows: **Firstly**, Alice will choose a prime p and $x_0, x_1 \in \mathbb{Z}_p^*$, and give them to Bob. **Secondly**, Bob will choose secret encryption and decryption exponents $e, d \in \mathbb{Z}_{p-1}$ such that $e \cdot d \equiv 1 \mod p-1$, encrypt x_i as $y_i \equiv x_{\pi(i)}^e \mod p$, where $0 \leq i \leq 1$ and either $\pi(i) = i$ or $\pi(i) = 1 - i$ for all i, and return y_0, y_1 to Alice. **Finally**, Alice will pick one of the ciphertexts $y \in \{y_0, y_1\}$ and Bob will reveal his decryption exponent d. Alice will win if $y^d \equiv x_0 \mod p$.

a) Given $p = 138547$, explain which (if any) of 25 or 26 would be a suitable choice for Bob's secret exponent e and compute its corresponding decryption exponent d.

b) Suppose that Alice "cheated" by choosing a Quadratic Residue (Q.R.) modulo 138547 for x_0 and a Quadratic non Residue (Q.n.R.) for x_1, and is given $y_0 = 45826$ and $y_1 = 57331$. Explain which one she should choose to avoid doing the dishes. (Assume Bob is honest.) [Hint: Examine how quadratic reciprocity is affected by encryption.]

c) Bob anticipates Alice's "cheating" by requiring that both x_0 and x_1 are either Q.R.s or Q.n.R.s. Explain why he is still not safe if computing discrete logarithms in $\mathbb{Z}_p^*$ is feasible.

Problem 2 During encryption with AES, the SubBytes operation substitutes byte $b = (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0) \in \mathbb{Z}_2^8$ with byte $c = (c_7, c_6, c_5, c_4, c_3, c_2, c_1, c_0) \in \mathbb{Z}_2^8$ via the affine map

$$\sigma(b) = (x^4 + x^3 + x^2 + x + 1) \cdot b_*(x) + (x^6 + x^5 + x + 1) \mod (x^8 + 1) \ ,$$

where $b(x) = \sum_{i=0}^{7} b_i x^i \in \mathbf{F} = \mathbb{Z}_2[x]/[x^8 + x^4 + x^3 + x + 1]$, $b^{-1}(x) \in \mathbf{F}$, $b_*(x)$ is the polynomial $b^{-1}(x)$ viewed as a polynomial in $\mathbb{Z}_2[x]$ instead of an element of $\mathbf{F}$ and $\sum_{i=0}^{7} c_i x^i = \sigma(b)$.

a) Find the byte c corresponding to byte $b = (1, 1, 0, 0, 1, 0, 1, 0)$.

b) Explain how AES encryption will be affected if $\mathbf{F} = \mathbb{Z}_2[x]/[x^8 + x^4 + x^3 + 1]$ instead. [Hint: For $g(x) = x^8 + x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$, what is $g(1)$ equal to and what does it mean?]

Problem 3 Alice and Bob are about to establish a secret key using the Diffie-Hellman key agreement protocol. Alice told Bob that they should use her birthdate which, given in the form DDMMYY, is a prime, and 7 which is a primitive element modulo this prime.

a) Bob doesn't remember if Alice's birthdate is 151187 or 151189. He is afraid she might be upset if he asked her and so he uses the Sollovay-Strassen test to find out. Despite that the first number is identified as being composite by the test, he tries to factor it to be sure. Is his uncertainty justified? He uses Pollard's $p - 1$ method with bound $B = 6$. Use the same method to find a factor of that number. [Hint: $a^2 \equiv (n - a)^2 \mod n$.]

b) Bob sends $h = 82935$ to Alice. Eve, who knows Alice's birthdate and thus $p = 151189$, sees this and tries to determine $\alpha = \log_7 h$ using the Pohlig-Hellman algorithm. Given that during her computations she obtained the following congruences, proceed to find α:

$$\begin{array}{rrll} 223 \cdot 113 \equiv & 1 & \text{mod } 293 & (1) \\ \alpha \equiv & 270 & \text{mod } 293 & (2) \\ \alpha \equiv & 4 & \text{mod } 43 & (3) \\ 30^{-1} \equiv & 33 & \text{mod } 43 & (4) \end{array}$$

$$\begin{array}{rrrll} 119840^{37797} \equiv & 7^{75594} & \equiv h^{75594} & \text{mod } p & (5) \\ 7^{50396} \not\equiv & 7^{100792} & \equiv h^{50396} & \text{mod } p & (6) \\ & 7^{151187} & \equiv 43197 & \text{mod } p & (7) \end{array}$$

Problem 4 Bob sent "The shares are low. Shall I buy? Yes or No?" unencrypted to Alice.

a) Alice wants to keep her "Yes" or "No" answer secret to anyone but Bob and will therefore encrypt it using a public key cryptosystem before sending. Explain why textbook RSA is not suitable for this situation, whereas her decision to use ElGamal could be reasonable.

b) Bob's public prime is $p = 23719$, "Yes" is encoded as 17173 and "No" as 6546. Alice sent her ElGamal-encrypted answer as $(5844, 1279) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$, but forgot to sign it. Explain how Eve, who knows the encoding used, is able to alter the ciphertext in a way that it decrypts to the opposite of the original plaintext, without computing discrete logarithms (that is, if Alice had encrypted "Yes", after Eve's interference the ciphertext will decrypt to "No", and vice versa). [Hint: Determine the conditions under which this can occur.]