NTNU – Trondheim
Norwegian University of
Science and Technology

Department of Mathematical Sciences

Examination paper for **TMA4160 Cryptography – solutions**

Academic contact during examination: Anders S. Lund

Phone: 73 59 16 25 / 41 45 19 15

Examination date: 10 December 2014

Examination time (from–to): 09:00–13:00

Permitted examination support material: B: All printed and hand-written support material is allowed. A specific basic calculator is allowed.

Other information:
All answers must be justified.

Language: English

Number of pages: 6

Number pages enclosed: 0

Checked by:

Date Signature

Problem 1 (10%) Calculate the Jacobi symbol $\left(\frac{2345}{6789}\right)$.

$$\begin{aligned}\left(\frac{2345}{6789}\right) &= \left(\frac{6789}{2345}\right) = \left(\frac{2099}{2345}\right)\\ &= \left(\frac{2345}{2099}\right) = \left(\frac{246}{2099}\right)\\ &= \left(\frac{2}{2099}\right)\left(\frac{123}{2099}\right) = -\left(-\left(\frac{2099}{123}\right)\right)\\ &= \left(\frac{8}{123}\right) = (-1)^3 = -1\end{aligned}$$

Answer: $\left(\frac{2345}{6789}\right) = -1$

Problem 2 (10%) Suppose we use the following formula to calculate MACs (Message Authentication Codes).

$$\text{Poly-MAC}(m) = a + bm \pmod{1249}$$

where a and b are positive integers less than 1249. 1249 is a prime.

Explain why this MAC is secure if it is used on only one message, but insecure if it is used on two or more messages.

Given one message, and secret random a and b, then any number less than 1249 is equaly likely. Therefore you cannot tell anything about a or b, and hence Poly-MAC is secure since you cannot forge a new MAC.

Now suppose you have used Poly-MAC on at least two messages m_1 and m_2, $m_1 \neq m_2$. Let c_1 =Poly-MAC(m_1) and c_2 =Poly-MAC(m_2). Then $c_1 - c_2 = b(m_1 - m_2)$ and $m_1 - m_2$ is invertible since 1249 is a prime, so you obtain b. Given m_1, c_1 (or m_2, c_2) and b, a is easy to calculate.

Problem 3 Let $p = 1249$, $g = 2$ and $h = 30$. You can still use that 1249 is a prime.

a) (10%) Use that $(g^{10}h^{-4})^4(g^{14}h^{15})^2(g^{157}h^{-19}) \equiv 1 \pmod{1249}$ to find $\log_g h$.

$$\begin{aligned} 1 &\equiv (g^{10}h^{-4})^4(g^{14}h^{15})^2(g^{157}h^{-19}) \\ &= g^{40}h^{-16}g^{28}h^{30}g^{157}h^{-19} \\ &= g^{68+157}h^{-5} \\ &= g^{225}h^{-5} \end{aligned}$$

So $g^{225}h^{-5} = 1$, meaning $g^{225} = h^5$. Using the extended Eucleadian algorithm one can compute that $5^{-1} \equiv 749 \pmod{1248}$, so $h = g^{225 \cdot 749}$, meaning $\log_g h \equiv 225 \cdot 749 \equiv 45 \pmod{1248}$.

Answer: $\log_g h = 45$.

b) (10%) Let (p, g, h) be a verification key for an ElGamal signature protokol. Use the answer in a) to find a signature on $m = 4$ with random key $k = 5$.

If you have not solved a), make a signature on $m = 4$ with $h = 79$, $a = 40$ and $k = 5$.

Assuming you use $h = 30$ (and hence $a = 45$):

$$\begin{aligned} \gamma &\equiv 2^k \equiv 2^5 \equiv 32 \pmod{1249}. \\ \delta &\equiv (m - a\gamma)k^{-1} \equiv (4 - 45 \cdot 32)5^{-1} \\ &\equiv (-1276) \cdot 749 \equiv 1060 \cdot 749 \\ &\equiv 212 \pmod{1248}. \end{aligned}$$

Assuming you use $h = 79$ (and hence $a = 40$):

$$\begin{aligned} \gamma &\equiv 2^k \equiv 2^5 \equiv 32 \pmod{1249}. \\ \delta &\equiv (m - a\gamma)k^{-1} \equiv (4 - 40 \cdot 32)5^{-1} \\ &\equiv (-1436) \cdot 749 \equiv 1220 \cdot 749 \\ &\equiv 244 \pmod{1248}. \end{aligned}$$

Answer: $h = 30$: $(\gamma, \delta) = (32, 212)$, $h = 79$: $(\gamma, \delta) = (32, 244)$.

Problem 4 Let $E : y^2 = x^3 + x + 1$ be an elliptic curve over the field $\mathbb{F}_{23}$. $P = (1, 7)$ and $Q = (11, 3)$ are points on the curve, and $Q = aP$ for some integer a. It is known that $2Q = (4, 0)$.

a) (10%) Suppose we are going to use ElGamal on the curve. Let (P, Q) be the public key, and a the secret key. Find the encryption of $M = (6, 19)$ when the randomness is $t = 2$ (you can safely assume that M is a point on the curve).

To find the encryption we must first calculate $2P$, and then $2Q + M$.
$2P$:

$$\begin{aligned} \gamma &\equiv (3 \cdot 1^2 + 1)(2 \cdot 7)^{-1} \equiv (4)(14)^{-1} \equiv 4 \cdot 5 \equiv 20 \pmod{23} \\ x_{2P} &\equiv 20^2 - 1 - 1 \equiv 398 \equiv 7 \pmod{23} \\ y_{2P} &\equiv 20(1 - 7) - 7 \equiv 20 \cdot 17 - 7 \equiv 11 \pmod{23} \\ 2P &= (7, 11) \end{aligned}$$

$2Q + M$:

$$\begin{aligned} \gamma &\equiv (19 - 0)(6 - 4)^{-1} \equiv (19)(2)^{-1} \equiv 19 \cdot 12 \equiv 21 \pmod{23} \\ x_{2P} &\equiv 21^2 - 6 - 4 \equiv 431 \equiv 17 \pmod{23} \\ y_{2P} &\equiv 21(4 - 17) - 0 \equiv 21 \cdot (-13) \equiv 3 \pmod{23} \\ 2Q + m &= (17, 3) \end{aligned}$$

Answer: The encryption of M with (P, Q) as public key is $([7, 11], [17, 3])$.

b) (10%) The order of P is divisible by a prime number greater than 6. Find the order of P. Is E cyclic?

Hasse's theorem gives that $(23 + 1) - 2\sqrt{23} \approx 14,41 \leq \#E \leq (23 + 1) + 2\sqrt{23} \approx 33,60$. We see that Q has order 4 since $2Q$ is on the line $y = 0$, and we know that $Q = aP$ for some a. This means $|\langle P \rangle| = 4 \cdot k$ for some number k. Now, assuming a prime p greater than 6 divides the order of P we get that $|\langle P \rangle| = 4 \cdot 7 \cdot k' = 28 \cdot k'$ ($p = 11$ would give an order larger than any possible $\#E$). Combining the results we get that $|\langle P \rangle| = 28$ and that P generates the elliptic curve, hence it is cyclic.

Answer: The order of P is 28 and E is cyclic.

Problem 5 (10%) Suppose we are using ElGamal with public key (g, h, p) to encrypt messages, and that we use the version of ElGamal where $e_K(m) = (g^t, h^t g^m)$ for a randomly chosen t and a small message m of your own choice, e.g. $m = 2047$ or $m = 2048$.

Explain why we should not use the square-and-multiply algorithm to do the exponentiations.

Hint: Suppose you can trick someone to encrypt repeatedly, and that you can measure the time it takes.

Note that the binary expansion of 2047 is just 1's, while 2048 has just one 1, so they are very different as strings. The square-and-multiply algorithm does a little extra work for each 1 that appears in the binary representation of each exponent, hence if you measure the time of many different encryptions you will be able decide how many 1's and 0's are in the exponents.

(For a single encryption, this information would be hidden by the inpredicability of the random number. However, the information adds up if we can do it many times.)

Problem 6 (10%) Alice sets up an RSA cryptosystem with public key (n, e), and awaits an important message from Bob. Eve wants to find out what the message Alice receives from Bob is, and manages to obtain the encrypted message. In addition she has a huge advantage: She was allowed to choose a small set of messages that Bob could choose from, but not the precise message.

How can Eve guarantee that she is always able to decide which message Alice receives as long as Alice and Bob uses standard RSA? Could Bob do something to stop Eve from succeeding?

As long as the set is small, Eve can encrypt all the messages and then check which one is sent. Since RSA is deterministic (i.e., it does not include any randomness) Eve will be able to find out which message that was sent.

When it comes to if Bob can do something to stop Eve this is an open question. If you assume you cannot modify the scheme, then the answer is no. However, if we can include a padding scheme, we will be good. For instance, when Bob converts the text m to a number, he can first append a random string, e.g. *YESgosxdx*, and then encrypt. Alice should have no problem identifying the message, since the set of small messages was small anyway.

Both yes and no are acceptable answers (meaning you can get full score!) as long as you have argued well for your position.

Problem 7 Let $n = 99221$.

a) (10%) Factor n by finding x and y such that $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv y \pmod{n}$.

Hint: Find a y such that $y \not\equiv \pm 2 \pmod{n}$, but $y^2 \equiv 4 \pmod{n}$.

Using the hint, we need to find $y \not\equiv \pm 2 \pmod{n}$ such that $y^2 \equiv 4 \pmod{n}$. $n = 99221$ and if one checks $99225 (= 99221 + 4)$ is a square in $\mathbb{Z}$, that is $99225 = 315^2$. Using this one gets $n = (315-2)(315+2) = 313 \cdot 317$.

Answer: $n = 313 \cdot 317$.

Concider the following protocol between Alice and Bob.

1. Alice chooses an RSA-modulus $n = pq$ (p and q known to Alice, but not to Bob), a public key e, a message m and calculates $c \equiv m^e \pmod{n}$. Alice sends (n, e, c) to Bob.
2. Bob chooses an $x \in \mathbb{Z}_n$ and calculates $y \equiv x^2 \pmod{n}$. Bob sends y to Alice.
3. Alice finds a random z such that $z^2 \equiv y \pmod{n}$. Alice sends z to Bob.

b) (10%) Explain how Bob can find m with probability $1/2$, that he can not get a higher probability of succeeding and that Alice cannot stop him, or know if he finds m or not.

There are four possible solutions to $y \equiv x^2 \pmod{n}$. Two of these solutions are $\pm x$ as chosen by Bob, which will not help him factor n. The two other solutions will make Bob able to factor n, and then decrypt using this information. Alice has no way of knowing which x Bob chose, hence has 50% chance of picking $\pm x$ and 50% chance of not picking $\pm x$, meaning that Bob has 50% chance of finding m (succeeding). Alice, having to follow the protocol, has no way to choose z such that Bob is guaranteed to not succeed (since y gives no information about x) and also by the same argument she cannot know if Bob succeeded (got m) or not. The interested reader should look up Rabin's oblivious transfer scheme.