NTNU

Norwegian University of
Science and Technology

Department of Mathematical Sciences

Examination paper for **TMA4160 Cryptography**

Academic contact during examination: Herman Galteland

Phone: 988 96 131

Examination date: December 14 2017

Examination time (from–to): 15:00-19:00

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

Other information:

Language: English

Number of pages: 3

Number of pages enclosed: 0

Checked by:

Informasjon om trykking av eksamensoppgave	
Originalen er:	
1-sidig ☐	**2-sidig** ☒
sort/hvit ☒	**farger** ☐
skal ha flervalgskjema ☐	

Date Signature

Problem 1 We have that $p = 271$ is a prime, that g is a generator for $\mathbb{F}_p^*$ and $x \in \mathbb{F}_p^*$.

a) You observe that $g^{147}x^3 = 1$. What do you know about $\log_g x$?

Let $g = 6$ and $x = 51$.

b) Use the Pohlig-Hellman algorithm to compute $\log_g x$.

c) Use Shanks' Baby-step Giant-step algorithm to compute $\log_g x$.

Note: You may not use information from one of the above problems to simplify the solution of the other three problems. However, the answers should be consistent, and you may use information from the other problems to check your answers.

Problem 2 Consider the elliptic curve $E : Y^2 = X^3 + 2X + 9$ defined over $\mathbb{F}_{19}$. The curve has 23 rational points and the points $P = (3, 17)$, $Q = (17, 15)$ and $R = (14, 8)$ all lie on the curve.

a) Show that $5P + 2R = \mathcal{O}$.

Hint: You may use that $4P = (6, 16)$.

b) Suppose you also know that $7P + 3R + 4Q = \mathcal{O}$. Find $\log_P Q$.

Problem 3 In this problem, we are going to talk about *blind signatures*. The point of blind signatures is that Bob has a signing key. Alice would like Bob to sign her message, and Bob is willing to sign her message. However,

- Alice does not want Bob to know what her message is; and
- Bob does not want Alice to get signatures on more than one message.

(This may sound crazy, but blind signatures are useful in areas such as elections and financial systems.)

a) We can use a variant of RSA signatures to create blind signatures. Let h be a suitable hash function. Bob creates his signing key $sk = (n, d)$ and verification key $vk = (n, e)$ as usual for RSA. An integer $0 \leq \sigma \leq n$ is a valid signature on a message m if $\sigma^e \equiv h(m) \pmod{n}$.

To get a signature on a message m

- Alice chooses a random number $0 < r < n$ (such that $\gcd(r, n) = 1$) and computes $t = r^e h(m) \bmod n$. She sends t to Bob.
- Bob computes $\tau = t^d \bmod n$. He sends τ to Alice.
- Alice computes $\sigma = \tau r^{-1} \bmod n$.

Show that σ as computed is a valid signature on m.

Explain why Bob learns nothing about m during this exchange.

We could also try to use a variant of Rabin signatures. In this case, we consider RSA moduluses like the following: Let p and q be large primes such that $(p-1)/2$ and $(q-1)/2$ are also prime. Let $n = pq$.

b) Show that any square modulo n has order dividing $(p-1)(q-1)/4$.

Suppose z is a square modulo n. Show that Bob (who knows p and q) can easily compute a square root of z modulo n.

c) Suppose x is a number such that the Jacobi symbol $\left(\frac{x}{n}\right) = 1$. Show that either x or $-x$ is a square modulo n.

Bob's verification key will be n, and Bob's secret key will be (p, q).

Bob also needs a special hash function h_n such that for all messages m with $y = h_n(m)$, the Jacobi symbol $\left(\frac{y}{n}\right) = 1$. (You do not need to consider how to construct such a hash function.)

d) An integer σ is a valid signature on a message m if $\sigma^2 \equiv \pm h_n(m) \pmod{n}$.

To get a signature on a message m

- Alice chooses a random number $0 < r < n$ such that $\gcd(r, n) = 1$ and the Jacobi symbol $\left(\frac{r}{n}\right) = 1$ and computes $t = r^2 h_n(m) \bmod n$. She sends t to Bob.
- Bob computes τ such that $\tau^2 \equiv \pm t \pmod{n}$. He sends τ to Alice.
- Alice computes $\sigma = \tau r^{-1} \bmod n$.

Show that σ as computed is a valid signature on m.

Explain how Alice can cheat to recover p and q with high probability, and thereby get signatures on any number of messages of her choice.

Problem 4 In this problem, we shall consider *Lamport's one-time signatures*. This scheme is interesting because it is very fast and it relies only on a one-way hash function. Let $h : S \to T$ be a hash function.

To create her key pair, Alice chooses n pairs of values $(a_{1,0}, a_{1,1}), (a_{2,0}, a_{2,1}), \ldots, (a_{n,0}, a_{n,1})$ from S at random. She computes n pairs of values $(x_{1,0}, x_{1,1}), (x_{2,0}, x_{2,1}), \ldots, (x_{n,0}, x_{n,1})$ as $x_{i,b} = h(a_{i,b})$. Her verification key is $vk = ((x_{1,0}, x_{1,1}), (x_{2,0}, x_{2,1}), \ldots, (x_{n,0}, x_{n,1}))$, her signing key is $sk = ((a_{1,0}, a_{1,1}), (a_{2,0}, a_{2,1}), \ldots, (a_{n,0}, a_{n,1}))$.

The signature on a message $(m_1, m_2, \ldots, m_n) \in \{0,1\}^n$ is $(a_{1,m_1}, a_{2,m_2}, \ldots, a_{n,m_n})$.

To verify a signature $(z_1, z_2, \ldots, z_n)$ on a message $(m_1, m_2, \ldots, m_n)$, Bob checks that $h(z_i) = x_{i,m_i}$, $i = 1, 2, \ldots, n$.

Suppose Alice signs the two messages $(m_1, \ldots, m_n)$ and $(m'_1, \ldots, m'_n)$ that differ in at least two positions. Explain how Eve can use these two signatures to create a forged signature on a third message $(m''_1, \ldots, m''_n)$.