Our final exam will have somewhat more emphasis on the later material of the course (i.e. post-midterm)

THE UNIVERSITY OF CALGARY

DEPARTMENT OF COMPUTER SCIENCE
DEPARTMENT OF MATHEMATICS AND STATISTICS

FINAL EXAMINATION

CPSC 418/MATH 318 L01 Introduction to Cryptography Fall 2018

December 12, 2018 19:00 - 22:00 Time: 3 hours

I.D. NUMBER	SURNAME	OTHER NAMES

COURSE (circle one): CPSC 418 MATH 318

STUDENT IDENTIFICATION

Each candidate must sign the Seating List confirming presence at the examination. All candidates for final examinations are required to place their University of Calgary student I.D. cards on their desks for the duration of the examination. Students without an I.D. card who can produce an **acceptable** alternative I.D., e.g., one with a printed name and photograph, are allowed to write the examination.

A student without acceptable I.D. will be required to complete an Identification Form. The form indicates that there is no guarantee that the examination paper will be graded if any discrepancies in identification are discovered after verification with the student's file. **A student who refuses to produce identification or who refuses to complete and sign the Identification Form is not permitted to write the examination.**

EXAMINATION RULES

1. Students late in arriving will not normally be admitted after one-half hour of the examination time has passed.
2. No candidate will be permitted to leave the examination room until one-half hour has elapsed after the opening of the examination, nor during the last 15 minutes of the examination. All candidates remaining during the last 15 minutes of the examination period must remain at their desks until their papers have been collected by an invigilator.
3. All inquiries and requests must be addressed to supervisors only.
4. **Candidates are strictly cautioned against**:
   (a) speaking to other candidates or communicating with them under any circumstances whatsoever;
   (b) bringing into the examination room any textbook, notebook or memoranda not authorized by the examiner;
   (c) making use of calculators and/or portable computing machines not authorized by the instructor;
   (d) leaving answer papers exposed to view;
   (e) attempting to read other students' examination papers.

   The penalty for violation of these rules is suspension or expulsion or such other penalty as may be determined.
5. Discarded matter is to be struck out and not removed by mutilation of the examination paper.
6. Candidates are cautioned against writing on their exam paper any matter extraneous to the actual answering of the question set.
7. The candidate is to write his/her ID number and name on the exam paper as directed.
8. During the examination a candidate must report to a supervisor before leaving the examination room.
9. Candidates must stop writing when the signal is given. Exam papers must be handed to the supervisor-in-charge promptly. Failure to comply with these regulations will be cause for rejection of an answer paper.
10. If during the course of an examination a student becomes ill or receives word of domestic affliction, the student must report at once to the supervisor, hand in the unfinished paper and request that it be cancelled. If physical and/or emotional ill health is the cause, the student must report at once to a physician/counsellor so that subsequent application for a deferred examination is supported by a completed Physical/Counsellor Statement form. Students can consult professionals at University Health Services or Counselling and Student Development Centre during normal working hours or consult their physician/counsellor in the community. **Once an examination has been handed in for marking, a student cannot request that the examination be cancelled for whatever reason. Such a request will be denied. Retroactive withdrawals will also not be considered.**

Problem	Topic	Total Marks	Actual Marks
1	Multiple Choice	10	
2	True/ False	10	
3	Definitions	11	
4	Short Answer	10	
5	Computations	16	
6	One-Time Pad	8	
7	Modes of Op'n	5	
8	Hash Functions	6	
9	Massey-Omura	7	
10	RSA	6+1	
11	ElGamal Sigs	13	
	Total	102+1	

INSTRUCTIONS

- This is a closed book exam. No aids are permitted; this includes calculators.
- Total marks: **102 + 1 bonus mark**. Score will be out of 100, so you can get up to **103%**.
- Answer all the questions in the space provided.
- Use the last 3 pages to continue answers if you need more space, or as rough paper.

1. **[10 marks] Multiple Choice Questions**

   For each question, check exactly one answer.

   (a) **1 mark**] Assuming that keys are chosen with equal likelihood, the shift cipher provides
   - ○ computational security
   - ● perfect secrecy
   - ○ semantic security
   - ○ none of the above

   (b) **1 mark**] The one-time pad is a
   - ● monoalphabetic substitution cipher
   - ○ polyalphabetic substitution cipher
   - ○ transposition cipher
   - ○ product cipher

   (c) **[1 mark]** Which of the following is true about AES?
   - ○ AES provides perfect secrecy
   - ○ AES is IND-CCA2 secure
   - ○ AES is GMR-secure
   - ● None of the above

   (d) **[1 mark]** Consider a block cipher with m-bit keys. Then the number of bits of security provided by double encryption $C = E_{K_1}(E_{K_2}(M))$ is approximately
   - ● m
   - ○ m^2
   - ○ $\sqrt{m}$
   - ○ None of the above

   (e) **[1 mark]** Which of the following cryptographic services is provided by message authentication codes?
   - ○ Confidentiality
   - ○ Non-repudiation
   - ○ Access control
   - ● None of the above

Multiple Choice Questions (cont'd)

(f) **[1 mark]** Which of the following applications can RSA ***not*** be used for?

- ○ Hybrid encryption
- ○ Authentication
- ○ Non-repudiation
- • RSA can be used for all of these applications

(g) **[1 mark]** Which of the following is true about the ElGamal public key cryptosystem?

- ○ It is randomized and signature capable
- • It is randomized but not signature capable
- ○ It is not randomized but signature capable
- ○ It is neither randomized nor signature capable

(h) **[1 mark]** What does is the role of a Key Distribution Centre?

- • To provide users with conventional cryptographic keys
- ○ To provide users with public/private key pairs
- ○ To oversee the execution of the Diffie-Hellman protocol between two users
- ○ To oversee the execution of the Station-to-Station protocol between two users

(i) **[1 mark]** Let $\left(\frac{\cdot}{\cdot}\right)$ denote the Jacobi symbol. Then the implication $\left(\frac{a}{n}\right) = 1 \implies a$ is a quadratic residue (mod n) holds

- ○ for all $n \in \mathbb{Z}$ with $n \geq 2$ and all $a \in \mathbb{Z}_n^*$
- ○ for all $n \in \mathbb{Z}$ with $n \geq 2$ and all $a \in \mathbb{Z}_n^*$ with n odd
- • for all $n \in \mathbb{Z}$ with $n \geq 2$ and all $a \in \mathbb{Z}_n^*$ with n prime
- ○ for all $n \in \mathbb{Z}$ with $n \geq 2$ and all $a \in \mathbb{Z}_n^*$ with n composite

(j) **[1 mark]** Suppose an adversary of a signature scheme can generate a valid signature to at least one message. Which of the following does she successfully execute?

- • Existential forgery
- ○ Selective forgery
- ○ Universal forgery
- ○ Finding the private key

2. **[10 marks] TRUE/FALSE Questions**

   Answer every questions with TRUE or FALSE. Just state your answer; no explanations are required.

   (a) **[1 mark]** The number of rounds in the Rijndael algorithm is independent of the key length. **FALSE**

   (b) **[1 mark]** Every block cipher can be converted to a stream cipher. **TRUE**

   (c) **[1 mark]** A block cipher used in cipher block chaining (CBC) mode is an example of a self-synchronous stream cipher. **FALSE**

   (d) **[1 mark]** Hybrid encryption is a combination of substitutions and transpositions. **FALSE**

   (e) **[1 mark]** 42 has an inverse modulo 90. **FALSE**

   (f) **[1 mark]** Let p be a prime and $g \in \mathbb{Z}_p^*$. If $g^{p-1} \equiv 1 \pmod{p}$, then g is a primitive root (mod p). **FALSE**, $g^{p-1} \equiv 1 \pmod{p}$ holds for all $g \in \mathbb{Z}_p^*$ by Fermat's Little Theorem.

   (g) **[1 mark]** Let $n = pq$ with distinct primes p, q, and let ϕ denote Euler's phi function. Then anyone with knowledge of n and $\phi(n)$ can efficiently find p and q. **TRUE**

   (h) **[1 mark]** A public key cryptosystem is polynomially secure if and only if it is IND-CCA2 secure. **FALSE**

   (i) **[1 mark]** The Station-to-Station protocol uses the challenge-response mechanism to provide mutual authentication. **TRUE**

   (j) **[1 mark]** In the Transport Layer Protocol of SSH, the client authenticates to the server. **FALSE**

3. **[11 marks] Definitions**

(a) **[2 marks]** Define a *chosen ciphertext attack* against a symmetric key cryptosystem.
Answer: The adversary chooses some ciphertext (independently of the ciphertext she wishes to decrypt) and obtains the corresponding plaintext.

(b) **[2 marks]** Let m be an integer with $m > 1$. Define the set Z_m^*.
Answer:

$$\begin{aligned} \mathbb{Z}_m^* &= \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\} \\ &= \{a \in \mathbb{Z} \mid 0 < a < m \text{ and } \gcd(a, m) = 1\} \end{aligned}$$

(c) **[2 marks]** Let m be a positive integer. Define the *Euler phi function* $\phi(m)$.
Answer: $\phi(m) = |\mathbb{Z}_m^*| = |\{a \in \mathbb{Z} \mid 0 < a < m \text{ and } \gcd(a, m) = 1\}|$

(d) **[3 marks]** Define what it means for a public key cryptosystem to be *polynomially secure*.
Answer: A PKC is said to be polynomially secure if no passive adversary can in expected polynomial time select two plaintexts M_1, M_2 and correctly distinguish between the encryptions of M_1 and M_2 with probability significantly greater than $1/2$.

(e) **[2 marks]** Explain the purpose of the certification authority in a public key infrastructure.
Answer: A certification authority is a trusted third party whose signature on a certificate vouches for the authenticity of the public key bound to the subject entity.

4. **[10 marks] Short Answer Questions**

   (a) **[2 marks]** Describe how a *substitution cipher* acts on plaintexts to convert them to ciphertexts.

   Answer: Encryption under a substitution cipher replaces each plaintext symbol by some ciphertext symbol without changing the order of the plaintext symbols.

   (b) **[2 marks]** Define what it means for a hash function to be *pre-image resistant*.

   Answer: Given any hash value x, it is computationally infeasible to find a pre-image of x, i.e. an input M for which $H(M) = x$.

   (c) **[2 marks]** Let p be a prime and g a primitive root of p. State the *Diffie-Hellman problem* in this setting.

   Answer: Given p, g, $g^a \pmod p$ and $g^b \pmod p$, find $g^{ab} \pmod p$.

   (d) **[2 marks]** State *Euler's Theorem*. Be sure to define or describe all your symbols.

   Answer: Let n be a positive integer and $a \in \mathbb{Z}_n^*$ (defined in Problem 3 (b)). Then $a^{\phi(n)} \equiv 1 \pmod n$ where ϕ is the Euler phi function as defined in Problem 3 (c).

   (e) **[2 marks]** Define a *pseudorandom bit generator*.

   Answer: A pseudorandom bit generator is an algorithmic technique for creating sequences of statistically random bits, initialized with a random seed.

5. **[16 marks] Simple Computations**

(a) **[3 marks]** Use the primitive root test to prove that 2 is a primitive root of 13. Answers that do not use the primitive root test will be penalized.

Answer: We need to show that $2^{(13-1)/q} \not\equiv 1 \pmod{13}$ for all prime factors q of $13-1$. Now $13-1 = 12 = 3 \cdot 2^2$, so the prime factors of 12 are 2 and 3.

$$2^{(13-1)/2} = 2^6 = 64 \equiv -1 \not\equiv 1(\pmod{13}) ,$$
$$2^{(13-1)/3} = 2^4 = 16 \equiv 3 \not\equiv 1 \pmod{13} .$$

(b) **[2 marks]** What is the discrete logarithm of 6 with respect to 2 modulo 13? Explain your answer.

Answer: It is the unique exponent x with $0 \leq x \leq 13-2$ such that $2^x \equiv 6 \pmod{13}$. By exhaustive search (trying 0, 1, 2, ...), we obtain

$$2^5 = 32 = 26 + 6 \equiv 6 \pmod{13} ,$$

so the discrete logarithm of 6 with respect to 2 modulo 13 is $x = 5$.

(c) **[3 marks]** Let

$$f(x) = x^2 + x + 1 , \quad g(x) = x^3 + x$$

be be polynomials with binary coefficients. Compute

$$f(x)g(x) \pmod{x^4 + x^2 + 1} .$$

Show your work.

Answer: Since $x^4 + x^2 + 1 \equiv 0 \pmod{x^4 + x^2 + 1}$, we have $x^4 \equiv x^2 + 1 \pmod{x^4 + x^2 + 1}$ and hence $x^5 \equiv x^3 + x \pmod{x^4 + x^2 + 1}$. Hence,

$$\begin{aligned} f(x)g(x) &= x^5 + x^4 + x^3 + x^3 + x^2 + x \\ &\equiv x^5 + x^4 + x^2 + x \\ &\equiv (x^3 + x) + (x^2 + 1) + x^2 + x \\ &\equiv x^3 + 1 \pmod{x^4 + x^2 + 1}. \end{aligned}$$

Simple Computations (cont'd)

(d) **[4 marks]** Find integers x, y such that $41x + 15y = 1$. Use any method you like except guessing, but show your work.
Answer:

$$\begin{aligned} 41 &= 2 \cdot 15 + 11 \\ 15 &= 1 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

So $\gcd(41, 15) = 1$ and we obtain

$$\begin{aligned} 1 &= 4 - 3 = 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 = 3(15 - 11) - 11 \\ &= 3 \cdot 15 - 4 \cdot 11 = 3 \cdot 15 - 4(45 - 2 \cdot 15) = 11 \cdot 15 - 4 \cdot 45 \ . \end{aligned}$$

Hence $x = -4$ and $y = 11$.

(e) **[3 marks]** Compute the Jacobi symbol $\left(\frac{26}{15}\right)$. Use any method you like, but show your work.
Answer: There are many ways to do this. The approach with the easiest arithmetic is probably to factor 15, reduce 26 modulo 3 and 5, and compute $(\frac{2}{3})$ directly:

$$\left(\frac{26}{15}\right) = \left(\frac{26}{3}\right)\left(\frac{26}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{5}\right) = (-1)^{(3^2-1)/8} \cdot 1 = -1 \ .$$

(f) **[1 mark]** Is 26 a quadratic residue modulo 15, a pseudosquare modulo 15, both, or neither? Just state your answer, no explanation necessary.
Answer: Neither, because $\left(\frac{26}{3}\right) = -1$ and $\left(\frac{26}{5}\right) = 1$.

6. **[8 marks] One-Time Pad**

   Consider the one-time pad applied to n bit blocks for some $n \in \mathbb{N}$, i.e. plaintext blocks, ciphertext blocks and keys are all bit strings of length n.

   (a) **[2 marks]** Describe the encryption and decryption procedures in this setting.
   Answer:
   - Encryption: $E_K(M) = M \oplus K$ for all $M, K \in \{0,1\}^n$ (bitwise x-or of M and K)
   - Decryption: $D_K(C) = C \oplus K$ for all $C, K \in \{0,1\}^n$.

   (b) **[2 marks]** Explain how an adversary who mounts a known plaintext attack can recover a secret one-time pad key.
   Answer: Given a plaintext $M \in \{0,1\}^n$ and a ciphertext $C \in \{0,1\}^n$, the key that encrypts M to C is $K = M \oplus C$ as $E_K(M) = M \oplus K = M \oplus (M \oplus C) = 0^n \oplus C = C$.

   (c) When using the one-time pad with the key $K = 0^n$ consisting of n zeros, we have $E_K(M) = M \oplus K = M$ for every message M, i.e. the message is sent unencrypted. It has been suggested to improve the one-time pad by only encrypting with non-zero keys.

      i. **[2 marks]** Use the *definition* of perfect secrecy,

      $$p(M) = p(M|C) \text{ for all messages } M \text{ and ciphertexts } C \text{ with } p(C) > 0 \ ,$$

      to prove that this modification of the one-time pad does not provide perfect secrecy. Answers that do not use this definition will receive at most half credit.
      Answer: Let $M \in \{0,1\}^n$ be any plaintext that actually occurs, so $p(M) > 0$, and put $C = M$. Then $p(C|M) = p(M|M) = 0$ as the only key that encrypts M to M is $K = 0^n$ which is excluded. Hence we have found a plaintext M and a ciphertext C such that $p(C|M) = 0 \neq p(M)$, which violates the definition of perfect secrecy.

      ii. **[2 marks]** Explain (informally) why allowing $K = 0^n$ does not weaken the security of the one-time pad, even though using that key does not change the plaintext when encrypting.
      Answer: Since the one-time pad has perfect secrecy, even when $C = M$, an adversary cannot verify that M really is the message since all messages are equally likely as decryptions of C.

7. **[5 marks] Modes of Operation**

   Let E_K denote encryption under some block cipher using the secret key K.

   (a) **[2 marks]** Describe how the key stream is produced when using the block cipher in *counter mode*.

   Answer $KS_i = E_K(CTR_i)$, $i = 1, 2, \ldots$ where E_K is encryption under the block cipher using key K and CTR_i is a counter such that $CTR_{i+1} = CTR_i + 1$ for all $i \in \mathbb{N}$.

   (b) **[2 marks]** Describe the encryption and decryption procedures when using the block cipher in counter mode.

   Answer: The encryption of the i-th message block $m_i \in \{0,1\}^n$ is $C_i = M_i \oplus KS_i$. The decryption of C_i is $M_i = C_i \oplus KS_i$.

   (c) **[1 mark]** Is a block cipher in counter mode a synchronous or a self-synchronizing stream cipher? Just state you answer, no explanation necessary.

   Answer: It is a synchronous stream cipher. At every step, the state depends only on the previous state (i.e. CTR_i is derived from CTR_{i-1} via an increment of 1), but it does not depend on the input M_i.

8. **[6 marks] Hash Functions**

Let $h : \{0,1\}^* \to \{0,1\}^n$ be an n-bit cryptographic hash function ($n \in \mathbb{N}$). Consider the following new hash function $H : \{0,1\}^* \to \{0,1\}^n$ derived from h as follows (as usual, "$\|$" denotes concatenation):

Input: $M \in \{0,1\}^*$

Output: An n-bit hash of M

Algorithm:

1) Put $M' = M$ if M has even length and $M' = M\|0$ if M has odd length
2) Write $M' = M_0\|M_1$ where M_0 and M_1 have the same length
3) Output $H(M) = h(M_0) \oplus h(M_1)$

(a) **[2 marks]** Prove that H is not weakly collision resistant by exhibiting an explicit weak collision.

Answer: All that is needed is an input M of even length whose first and second half are different. Then a collision is given by swapping the first and second half of M.

An very simple explicit example is $M = 01$. Then $M_0 = 0$ and $M_1 = 1$, so

$$H(01) = h(0) \oplus h(1) = h(1) \oplus h(0) = H(10) \ .$$

Since $01 \neq 10$, this constitutes a weak collision for $M = 01$.

Another simple answer is to just chose any M of odd length (e.g. $M = 0$), because then $M \neq M\|0$. but $H(M) = H(M\|0)$.

(b) **[2 marks]** Is H is strongly collision resistant? Explain.

Answer: No because every strongly collision resistant hash function is also weakly collision resistant. Since H is not weakly collision resistant, it is also not strongly collision resistant.

(c) **[2 marks]** Prove that H is not pre-image resistant by exhibiting a pre-image of 0^n under H.

Answer: Here, all that is needed is an input M of even length whose first and second half are identical, e.g. $M = 00$. Any such string is a pre-image of 0^n under H. To see this, write $M = M_0\|M_0$. Then $H(M) = h(M_0) \oplus h(M_0) = 0^n$.

The message $M = 0$ is also a pre-image of 0^n as $M' = 00$ in this case, which yields the previous example.

9. **[7 marks] Massey-Omura Cryptosystem**

In this (*conventional, not public key!*) cryptosystem, all users agree on a large public prime p. Each user U has a secret key which is a pair (e_U, d_U) with $e_U, d_U \in \mathbb{Z}_{p-1}^*$ such that

$$e_U d_U \equiv 1 \pmod{p-1} .$$

Messages are elements of Z_p^*.

Consider two users Alice with key (e_A, d_A) and Bob with key (e_B, d_B). If Alice wishes to send an encrypted message $M \in \mathbb{Z}_p^*$ to Bob, she proceeds as follows:

Step 1: Alice sends $C_A \equiv M^{e_A} \pmod{p}$ to Bob.
Step 2: Bob sends $C_B \equiv C_A^{e_B} \pmod{p}$ to Alice.
Step 3: Alice sends $M_A \equiv C_B^{d_A} \pmod{p}$ to Bob.
Step 4: Bob computes $M \equiv M_A^{d_B} \pmod{p}$.

(a) **[3 marks]** Formally prove that $M_A \equiv M^{e_B} \pmod{p}$.
Answer: For brevity, put $X = M^{e_B}$. Then

$$M_A \equiv C_B^{d_A} \equiv (C_A^{e_B})^{d_A} \equiv ((M^{e_A})^{e_B})^{d_A} \equiv (M^{e_B})^{e_A d_A} \equiv X^{e_A d_A} \pmod{p} .$$

By construction, $e_A d_A = 1 + k(p-1)$ for some $k \in \mathbb{Z}$, so

$$X^{e_A d_A} \equiv X^{1+k(p-1)} \equiv X(X^k)^{p-1} \equiv X \pmod{p} ,$$

so $M_A \equiv X \equiv M^{e_B} \pmod{p}$.

(b) **[1 mark]** Which mathematical theorem is used to prove the result of part (a)? You need not state the theorem, just its name.
Answer: Fermat's Little Theorem. It is used for the last congruence in the previous equation display.
Euler's Theorem is also an acceptable answer, since Fermat's Little Theorem is a special case of that.

(c) **[3 marks]** Use the result of part (a) to prove that this cryptosystem works, i.e. that Bob in step 4 does indeed obtain the message M sent by Alice.
Answer: In step 4, Bob computes $M_A^{d_B} \pmod{p}$; the claim is that this is the original message M. From part (a), we obtain

$$M_A^{d_B} \equiv (M^{e_B})^{d_B} \equiv M^{e_B d_B} \pmod{p} .$$

As in the proof of part (a), write $e_B d_B = 1 + n(p-1)$ for some $n \in \mathbb{Z}$, so

$$M^{e_B d_B} \equiv M^{1+n(p-1)} \equiv M(M^n)^{p-1} \equiv M \pmod{p} ,$$

so $M_A^{d_B} \equiv M \pmod{p}$ as claimed.

10. **[6 marks plus 1 bonus mark] RSA**

Consider an RSA user Alice with public key (e, n) and private key d. Consider the (incomplete) description below of the adaptive chosen ciphertext attack against Alice covered in class that exploits the multiplicative property of RSA. To obtain the decryption M of a given ciphertext C, an attacker Mallory proceeds as follows:

Step 1: Generates some $X \in \mathbb{Z}_n^*$
Step 2: Computes a suitable ciphertext C' from C and X (this is her chosen ciphertext)
Step 3: Obtains the decryption M' of C'
Step 4: Computes M from M' and X

(a) **[2 marks]** Explain how Mallory computes C' from C and X in step 2.

Answer: $C' \equiv CX^e \pmod{n}$ (need $X^e \not\equiv 1 \pmod{n}$ to ensure $C' \neq C$; otherwise Mallory is not permitted to send C' for decryption).

(b) **[2 marks]** Explain how Mallory computes M from M' and X in step 4. Prove this computation does in fact yield M.

Answer: Let Y be the inverse of X modulo n, so $XY \equiv 1 \pmod{n}$. We claim that $M \equiv YM' \pmod{n}$. To see this, not that $C \equiv C'Y^e \pmod{n}$ and hence

$$M \equiv C^d \equiv (C')^d (Y^e)^d \equiv (C')^d Y^{ed} \equiv (C')^d Y \equiv M'Y \pmod{n} .$$

(c) **[1 mark + 1 bonus mark]** What is the acronym of the augmentation procedure used in conjunction with RSA to foil this attack? Answers that give the full name rather than just the acronym receive a bonus mark.

Answer: Optimal Asymmetric Encryption Padding (OAEP).

(d) **[1 mark]** Name the strongest security notion satisfied by this augmented version of RSA. Just state the name, no explanation required.

Answer: Plaintext awareness.

11. **[13 marks] ElGamal Signature Scheme**

Recall the ElGamal signature scheme where a signer Alice produces her public and private keys as follows:

Step 1: Selects a large prime p and a primitive root g of p
Step 2: Randomly selects x such that $0 < x < p-1$ and computes $y \equiv g^x \pmod{p}$
Step 3: Alice's public key is (p, g, y); her private key is x

Alice also fixes a public cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}_{p-1}^*$. She signs a message $M \in \{0,1\}^*$ as follows:

Step 1: Selects a random integer $k \in \mathbb{Z}_{p-1}^*$
Step 2: Computes $r \equiv g^k \pmod{p}$
Step 3. Solves $ks \equiv H(M\|r) - xr \pmod{p-1}$ for s
Step 4. Attaches the signature (r, s) to message M

Upon receipt of (M, r, s), a verifier verifies the signature as follows:

Step 1: Obtains Alice's public key (p, g, y).
Step 2: Computes $v_1 \equiv y^r r^s \pmod{p}$ and $v_2 \equiv g^{H(M\|r)} \pmod{p}$
Step 3: Accepts the signature if and only if $v_1 \equiv v_2 \pmod{p}$.

(a) **[3 marks]** Carefully prove that the verification procedure is correct, i.e. prove that $v_1 \equiv v_2 \pmod{p}$ if the signature was properly generated. Show all your work.

Answer: By signature generation step 3, there exists $n \in \mathbb{Z}$ such that $ks + xr = H(M\|r) + n(p-1)$. Hence, from signature verification step 2:

$$\begin{aligned} v_1 &\equiv y^r r^s \equiv (g^x)^r (g^k)^s \equiv g^{xr+ks} \equiv g^{H(M\|r)+n(p-1)} \\ &= g^{H(M\|r)} (g^n)^{p-1} \equiv g^{H(M\|r)} \equiv v_2 \pmod{p} \ . \end{aligned}$$

(b) **[2 marks]** Name and state a mathematical problem on whose presumed intractability the security of the ElGamal signature scheme is based.

Answer: Discrete Logarithm Problem: given g and $g^x \pmod{p}$ for some $x \in \{0, , \ldots, p-2\}$, compute x.

ElGamal Signature Scheme (cont'd)

(c) Suppose Alice uses the same random number k to sign two different messages, i.e. she produces signatures (r, s_1) to a message M_1 and (r, s_2) to a message M_2 (note that the first component r of both signatures is the same when the same random number k is used for both signatures).

i. **[3 marks]** Assuming that $\gcd(s_1 - s_2, p-1) = 1$, carefully explain how an adversary who intercepts (M_1, r, s_1) and (M_2, r, s_2) can efficiently recover k.
Answer: From signature generation step 3, we have

$$ks_1 \equiv H(M_1\|r) - xr \pmod{p-1}$$
$$ks_2 \equiv H(M_2\|r) - xr \pmod{p-1} .$$

Subtracting the second from the first of these two congruences yields

$$k(s_1 - s_2) \equiv H(M_1\|r) - H(M_2\|r) \pmod{p-1} .$$

The adversary knows the right hand side of this congruence (since M_1, M_2 and r are intercepted and H is public). Since $\gcd(s_1 - s_2, p-1) = 1$ by assumption, the adversary can easily deploy the extended Euclidean algorithm to compute the modular inverse s of $s_1 - s_2 \pmod{p-1}$. Then

$$(s_1 - s_2)s \equiv 1 \pmod{p-1} ,$$

and hence

$$k \equiv (H(M_1\|r) - H(M_2\|r)s \pmod{p-1} .$$

ii. **[2 marks]** Assuming in addition that $\gcd(r, p-1) = 1$, prove how knowledge of k allows the attacker to efficiently recover Alice's private key x.
Answer: From signature generation step 3, we have $xr = H(M_1\|r) - ks_1 \pmod{p-1}$. The adversary knows the right-hand side of this congruence as well as r. Since $\gcd(r, p-1) = 1$ by assumption, the adversary can easily deploy the extended Euclidean algorithm to compute the modular inverse t of $r \pmod{p-1}$. Then

$$x \equiv (H(M_1\|r) - ks_1)t \pmod{p-1} .$$

(d) **[3 marks]** Suppose Alice chooses $p = 13$, $g = 2$ and $x = 11$ (by Problem 5 (a), 2 is a primitive root modulo 13). Use the binary exponentiation algorithm covered in class to compute Alice's corresponding public key value y. Solutions that do not use this algorithm will be penalized and may receive no credit.
Answer: The binary representation of $x = 11$ is 1011. With the notation in class, we obtain $b_0 = 1$, $b_1 = 0$, $b_2 = b_3 = 1$. Thus,

$$r_0 = g = 2 ,$$
$$r_1 \equiv g^{b_1} r_0^2 \equiv r_0^2 \equiv 2^2 \equiv 4 \pmod{13} ,$$
$$r_2 \equiv g^{b_2} r_1^2 \equiv g r_1^2 \equiv 2 \cdot 4^2 \equiv 2 \cdot 16 \equiv 2 \cdot 3 \equiv 6 \pmod{13} ,$$
$$r_3 \equiv g^{b_3} r_1^2 \equiv g r_2^2 \equiv 2 \cdot 6^2 \equiv 2 \cdot 36 \equiv 2 \cdot 10 \equiv 20 \equiv 7 \pmod{13} .$$

Thus, $y = 7$.

End of Solution Key ********** RS / rs