Sample Midterm Review

November 5, 2019

Problem 1 Background

Alice and Bob use an alphabet with 17 letters. Hence their alphabet can be viewed as $\{0, \ldots, 16\}$ with arithmetic mod 17. Answer the following questions and briefly explain why your answer is correct.

Problem 1a

(Alice and Bob are using alphabet $\{0, \ldots, 16\}$.) Alice and Bob want to use the affine cipher and they INSIST that $a \neq 0$. Give three ordered pairs (a, b) (with $a \neq 0$) such that the affine cipher x goes to $ax + b$ CAN be used, or state (no proof needed) that there is no such pair.

Problem 1a

(Alice and Bob are using alphabet $\{0, \ldots, 16\}$.) Alice and Bob want to use the affine cipher and they INSIST that $a \neq 0$. Give three ordered pairs (a, b) (with $a \neq 0$) such that the affine cipher x goes to $ax + b$ CAN be used, or state (no proof needed) that there is no such pair.

ANSWER

We list ALL of the (a, b) that work

$$\{(a, b) \;\; 1 \leq a \leq 16 \text{ and } 0 \leq b \leq 16\}$$

This works since ALL of the $1 \leq a \leq 16$ are rel prime to 17.

Problem 1b

(Alice and Bob are using alphabet $\{0, \ldots, 16\}$.) Alice and Bob want to use the affine cipher and they INSIST that $a \neq 0$. Give three ordered pairs (a, b) (with $a \neq 0$) such that the affine cipher x goes to $ax + b$ CANNOT be used, or state (no proof needed) that there is no such pair.

Problem 1b

(Alice and Bob are using alphabet $\{0, \ldots, 16\}$.) Alice and Bob want to use the affine cipher and they INSIST that $a \neq 0$. Give three ordered pairs (a, b) (with $a \neq 0$) such that the affine cipher x goes to $ax + b$ CANNOT be used, or state (no proof needed) that there is no such pair.

ANSWER

There are NO such (a, b) since all $1 \leq a \leq 16$ are rel prime to 17.

Problem 1c

(Alice and Bob are using alphabet $\{0, \ldots, 16\}$.) Alice and Bob want to use the matrix cipher and they INSIST that a, b, c, d all be BETWEEN 1 AND 10, AND ALL BE DIFFERENT. Give a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(with a, b, c, d all BETWEEN 1 AND 10 AND ALL DIFFERENT) such that it CAN be used for a 2×2 matrix cipher OR state (no proof needed) that no such matrix exists.

Problem 1c

(Alice and Bob are using alphabet $\{0, \ldots, 16\}$.) Alice and Bob want to use the matrix cipher and they INSIST that a, b, c, d all be BETWEEN 1 AND 10, AND ALL BE DIFFERENT. Give a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(with a, b, c, d all BETWEEN 1 AND 10 AND ALL DIFFERENT) such that it CAN be used for a 2×2 matrix cipher OR state (no proof needed) that no such matrix exists.

ANSWER

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Det is $4 - 6 = -2 \equiv 15$, rel prime to 17, so invertible.

Problem 1d

(Alice and Bob are still using alphabet $\{0, \ldots, 16\}$.) Alice and Bob want to use the matrix cipher and they INSIST that a, b, c, d all be BETWEEN 1 AND 10, AND ALL BE DIFFERENT (same as the last problem). Give a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(with a, b, c, d all BETWEEN 1 AND 10 AND ALL DIFFERENT) such that it CANNOT be used for a 2×2 matrix cipher OR state (no proof needed) that no such matrix exists.

Problem 1d

(Alice and Bob are still using alphabet $\{0, \ldots, 16\}$.) Alice and Bob want to use the matrix cipher and they INSIST that a, b, c, d all be BETWEEN 1 AND 10, AND ALL BE DIFFERENT (same as the last problem). Give a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

(with a, b, c, d all BETWEEN 1 AND 10 AND ALL DIFFERENT) such that it CANNOT be used for a 2×2 matrix cipher OR state (no proof needed) that no such matrix exists.

ANSWER

$$\begin{pmatrix} 2 & 10 \\ 1 & 5 \end{pmatrix}$$

Det is $2 \times 5 - 1 \times 10 = 0$, NOT rel prime to 17, so not invertible.

COMMON MISTAKES Students made in Fall 2018

1. Some students used numbers outside of $\{0, \ldots, 16\}$. NO! This is a mod 17 problem and the problem said only use $\{0, \ldots, 16\}$.
2. Some students thought that in the affine cipher a has to be rel prime to b. NO, a need only be rel prime to 17.
3. Some students thought that in the Matrix Cipher a, b, c, d have to be rel prime to each other. NO, we only need $ad - bc$ to be rel prime to 17.
4. In the problem where I said to have $a, b, c, d \in \{1, \ldots, 10\}$ some students had some of a, b, c, d over 11. Some had some of them equal. NO! The instructions said that a, b, c, d are BETWEEN 1 AND 10 AND ALL DIFFERENT.

Problem 2

Alice and Bob are doing Diffie-Hellman with $p = 11$ and $g = 2$

Problem 2a

If Alice picks $a = 3$ and Bob picks $b = 4$ then what is the shared secret? Alice computes $(2^4)^3 = 5^3 = 25 \times 5 \equiv 3 \times 5 = 15 \equiv 4$.

Problem 2a

If Alice picks $a = 3$ and Bob picks $b = 4$ then what is the shared secret? Alice computes $(2^4)^3 = 5^3 = 25 \times 5 \equiv 3 \times 5 = 15 \equiv 4$.

ANSWER

Alice computes $2^3 \equiv 8$.

Bob computes $2^4 \equiv 16 \equiv 5$.

Alice computes $(2^4)^3 = 5^3 = 25 \times 5 \equiv 3 \times 5 = 15 \equiv 4$.

Just to check

Bob computes $(2^3)^4 = 8^4 = 64 \times 64 \equiv -2 \times -2 \equiv 4$.

So secret is 4

Problem 2b

If Alice picks $a = 4$ and Bob picks $b = 3$ then what is the shared secret?

Problem 2b

If Alice picks $a = 4$ and Bob picks $b = 3$ then what is the shared secret?

ANSWER

Alice computes $2^4 \equiv 16 \equiv 5$.

Bob computes $2^3 \equiv 8$,

Alice computes $(2^3)^4 = 8^4 = 64 \times 64 \equiv -2 \times -2 \equiv 4$.

Just to check

Bob computes $(2^4)^3 = 5^3 = 25 \times 5 \equiv 3 \times 5 = 15 \equiv 4$.

So secret is 4.

Problem 2c

You should have gotten the same answer for the last two questions. Either prove or disprove the following statement

Assume Alice and Bob do Diffie Hellman with (p, g). *Let* $s_{x,y}$ *be the secret if Alice picks* x *and Bob picks* y. *Then* $s_{x,y} = s_{y,x}$.

Problem 2c

You should have gotten the same answer for the last two questions. Either prove or disprove the following statement

Assume Alice and Bob do Diffie Hellman with (p, g). *Let* $s_{x,y}$ *be the secret if Alice picks* x *and Bob picks* y. *Then* $s_{x,y} = s_{y,x}$.

ANSWER

Yes its true In the first case the secret is g^{xy}, in the second g^{yx}. But these are the same.

Key to understanding DE-Key Exchange We needed $xy = yx$. In the other versions of DE that I mentioned also had $xy = yx$. In the matrix version I showed you we instead used

$$(xy)z = x(yz)$$

COMMON MISTAKES Students made in Fall 2018

1. Some students left the answer as 2^{12}. or even $2^{12} \pmod{11}$. We have always calculated the actual number using repeated squaring – that's why repeated squaring is important.
2. Some students had the answer be something > 11. In Diffie-Hellman the answer is always in $\{1, \ldots, p-1\}$.
3. Some students made arithmetic mistakes. On a 5-point problem which is VERY EASY computationally on an exam with 0 time pressure (all but 10 people left 15 minutes early) that's worth 0 points.

Problem 3

For each of the following give BOTH an intelligent argument of why it is TRUE *and* an intelligent argument of why it is FALSE.

Problem 3a

When doing, RSA always use $e = 2^{16} + 1$.

Problem 3a

When doing, RSA always use $e = 2^{16} + 1$.

ANSWER

TRUE e is large enough to thwart off the low-e attacks,

TRUE Computing m^e takes only 15 mults. This is small since $2^{16} + 1$ only has one 1 in it.

TRUE e is prime and hence is likely to be relatively prime to R.

FALSE If you always use the same e then Eve can study that number REALLY INTENSELY and maybe find a way to exploit that.

FALSE What if you are Zelda and you are sending things out to over 66,000 people? Now the low-e attack will work.

Problem 3b

The Vig-Book Cipher is good to use.

Problem 3b

The Vig-Book Cipher is good to use.

ANSWER

TRUE The key is really long and if you use an obscure book, and Eve does not have sophisticated computers, its hard to break (You can mention Freq analysis will not work.)

FALSE If Eve has sophisticated computers and letters freq she can use freq of pairs of letters to crack.

FALSE You cannot use a common book like the bible. (You can always use *Problems with a Point* or *Bounded Queries in Recursion Theory* or *Muffin Mathematics Nobody wants a small piece*.)

Common Mistakes on Problem 3

1. Saying something FALSE. For example
   $2^{16}+1$ *may or may not be prime*
   Since book ciphers always use the Bible they are easily broken
2. Saying something about the cipher that is mostly FALSE. For example
   If the Book is longer than the message then the book cipher IS the 1-time pad
3. Saying something about RSA with $e = 2^{16}+1$ that is true for ANY choice of parameters for RSA. For example
   if $e = 2^{16}+1$ *then they do not need to meet*
4. Saying something about the Book Cipher that is true for ANY choice of parameters for RSA. For example
   If use Book Cipher they need to meet.
   True for ANY private key encryption.

Problem 4

Describe the Blum-Williams variant of the Rabin Encryption (also called Rabin 2.0 — in this variant, Alice can decrypt uniquely). You need not prove correctness or security. Your answer should be such that someone who has not had the course can understand and implement your protocol. Your answer should include

- What Alice does to initialize the encryption.
- What messages m Bob is allowed to send.
- What Bob does to encrypt m producing c.
- What Alice does to decrypt c.

Problem 4 Answer

Problem 4 Answer

ANSWER

Rabin-BW encryption

L is sec param.

1. Alice gen p, q primes of length L such that $p, q \equiv 3 \pmod 4$. Let $N = pq$. Send N.
2. Encode To send $m \in SQ_N$, Bob sends $c = m^2 \pmod N$.
3. Decode Alice can find 2 or 4 m such that $m^2 \equiv c \pmod N$. Take the $m \in SQ_N$.

Problem 5

In Rabin-BW $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$. Show what goes wrong if $p = 5$ and $q = 3$. You will needs

$1^2 \equiv 14^2 \equiv 1 \pmod{15}$

$2^2 \equiv 13^2 \equiv 4 \pmod{15}$

$3^2 \equiv 12^2 \equiv 9 \pmod{15}$

$4^2 \equiv 11^2 \equiv 1 \pmod{15}$

$5^2 \equiv 10^2 \equiv 10 \pmod{15}$

$6^2 \equiv 9^2 \equiv 6 \pmod{15}$

$7^2 \equiv 8^2 \equiv 4 \pmod{15}$

Problem 5

In Rabin-BW $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$. Show what goes wrong if $p = 5$ and $q = 3$. You will needs

$1^2 \equiv 14^2 \equiv 1 \pmod{15}$

$2^2 \equiv 13^2 \equiv 4 \pmod{15}$

$3^2 \equiv 12^2 \equiv 9 \pmod{15}$

$4^2 \equiv 11^2 \equiv 1 \pmod{15}$

$5^2 \equiv 10^2 \equiv 10 \pmod{15}$

$6^2 \equiv 9^2 \equiv 6 \pmod{15}$

$7^2 \equiv 8^2 \equiv 4 \pmod{15}$

ANSWER

Bob only sends squares, so Bob only sends $\{1, 4, 6, 9, 10\}$.

To send 1, Bob sends $1^2 \pmod{15} \equiv 1$.

Alice tries to decode. She finds the four sqrts of 1 $\{1, 4, 11, 14\}$.

In the normal BW-Rabin there would be only ONE element of this set that is a square, and thats the one that Alice knows was send.

But there are two 1 and 4. Hence Alice cannot decode uniquely.

Common Mistakes for Problem 5

Note that we can only encode elements of $\{1, 4, 6, 9, 10\}$. Some students gave an example where they encoded something NOT in that set.

Problem 6a

Plain RSA had the problem that message m always got encoded the same way. Describe how we modified RSA to overcome that problem. (ADDED LATER—this is what we call the NY,NY problem.)

Problem 6a

Plain RSA had the problem that message m always got encoded the same way. Describe how we modified RSA to overcome that problem. (ADDED LATER—this is what we call the NY,NY problem.)

ANSWER

Fixing Plain RSA Alice and Bob need to agree that the message m will be of length exactly L_1 and r will be of length exactly L_2. ($L_1 + L_2$ is max length allowed).

To send $m \in \{0,1\}^{L_1}$ rather than send m^e generate random $r \in \{0,1\}^{L_2}$ and send $(rm)^e$. NOTE- rm is r CONCAT m. Alice knows to decrypt and take the rightmost L_1 bits.

Problem 6b

Describe the Blum-Goldwasser encryption system.

1. Alice p, q primes len L, $p, q \equiv 3 \pmod 4$. $N = pq$. Send N.
2. Encode Bob sends $m \in \{0,1\}^M$ picks random $r \in \mathbb{Z}_N^*$
   $x_1 = r^2 \mod N \qquad b_1 = LSB(x_1)$.
   $x_2 = x_1^2 \mod N \qquad b_2 = LSB(x_2)$.
   $\vdots$
   $x_{M+1} = x_M^2 \mod N \qquad b_{M+1} = LSB(x_{M+1})$.
   Send $c = ((m_1 \oplus b_1, \ldots, m_M \oplus b_M), x_{M+1})$.
3. Decode Alice From x_{M+1} Alice can compute x_M, ..., x_1 by sqrt (can do since Alice has p, q). Then can compute $b_1, \ldots, b_M$ and hence $m_1, \ldots, m_M$.

Problem 6c- First Solution

Blum-Goldwasser has the same problem as RSA – message m always encodes the same way. Modify Blum-Goldwasser so that it no longer has this problem. (ITOT BG DID NOT have the same problem as RSA. So find to either fix BG or say why it does not need fixing)

Problem 6c- First Solution

Blum-Goldwasser has the same problem as RSA – message m always encodes the same way. Modify Blum-Goldwasser so that it no longer has this problem. (ITOT BG DID NOT have the same problem as RSA. So find to either fix BG or say why it does not need fixing)

ANSWER ONE

Fixing BG Alice and Bob need to agree that the message m will be of length exactly L_1 and r will be of length exactly L_2. (L_1, L_2 should be chosen so that their sum is close to the max length allowed.)

To send $m \in \{0,1\}^{L_1}$ rather than send $BG(m)$ generate random $r \in \{0,1\}^{L_2}$ and send $BG(rm)$. NOTE- rm is r CONCAT m. Alice knows to decrypt and take the rightmost L_1 bits.

Problem 6c– Second Solution

Problem 6c– Second Solution

ANSWER TWO Bill you're a moron!

Recall that BG already uses a random seed.

To send $m \in \{0,1\}^L$ Bob picks a *random* $r \in \mathbb{Z}_N$ and uses it to generate a psuedo-random sequence $b_1 \cdots b_L$ and sends $(m_1 \oplus b_1) \cdots (m_L \oplus b_L)$.

If he send m again he would *pick a different r and hence get a different psuedo-random sequence of bits.* Hence m send twice *already* does not encrypt to the same thing.

Common Mistakes on Problem6

1. For 6a, the padding is to CONCAT by a random string, not MULTIPLY. Some students multiplied.
2. For 6c, some students just STATED that BG does not have the same problem as RSA but did not say why.

Problem 7

Describe a variant of the 2×2 matrix cipher that such that Alice and Bob can verify that it has not been tampered with. Describe

- What the Key is.
- If Alice wants to send $(m_1, \ldots, m_n)$ what does she sends (we assume n is even).
- If Bob receives what Alice send, how does he decode it and make sure it came from Alice.

Problem 7 Answer

The key is a an invertible 2×2 matrix M (over mod 26) AND a function g from $\{0, \ldots, 25\}$ to $\{0, \ldots, 25\}$.
To send a message $m_1, \ldots, m_n$ (we assume n is even) Alice does the following

- For each odd i, computer $M(m_i, m_{i+1}) = (c_i, c_{i+1})$.
- For each $1 \leq i \leq n$ compute $d_i = g(m_i)$.
- Send

$$(c_1, d_1), (c_2, d_2), \ldots, (c_n, d_n)$$

For Bob to decode and authenticate
Bob gets $(c_1, d_1), \ldots, (c_n, d_n)$.

- For each odd i, computer $M(c_i, c_{i+1}) = (m_i, m_{i+1})$.
- For every $1 \leq i \leq n$ computers $g(m_i)$. If get d_i then know not tampered with. If EVERY don't get d_i then tampered with.