Final Review-Admin

1) Final is Saturday Dec 14 1:30-3:30 in IRB 0318.

Final Review-Admin

1) Final is Saturday Dec 14 1:30-3:30 in IRB 0318.

2) Can bring one sheet of notes.
Can: use both sides, type it, put what you want on it.
Can: copy a classmates, cram entire course–Bad Ideas
Can: cram THIS talk on it-Bad Idea

Final Review-Admin

1) Final is Saturday Dec 14 1:30-3:30 in IRB 0318.

2) Can bring one sheet of notes.
Can: use both sides, type it, put what you want on it.
Can: copy a classmates, cram entire course–Bad Ideas
Can: cram THIS talk on it-Bad Idea

3) No calculators allowed.

Final Review-Admin

1) Final is Saturday Dec 14 1:30-3:30 in IRB 0318.

2) Can bring one sheet of notes.
Can: use both sides, type it, put what you want on it.
Can: copy a classmates, cram entire course–Bad Ideas
Can: cram THIS talk on it-Bad Idea

3) No calculators allowed.

4) Coverage: Slides/HW. Comprehensive.
5) Not on Exam: LWE, Bridge Cheating, My Book Talk, NSA talk.

Final Review-Admin

1) Final is Saturday Dec 14 1:30-3:30 in IRB 0318.

2) Can bring one sheet of notes.
Can: use both sides, type it, put what you want on it.
Can: copy a classmates, cram entire course–Bad Ideas
Can: cram THIS talk on it-Bad Idea

3) No calculators allowed.

4) Coverage: Slides/HW. Comprehensive.
5) Not on Exam: LWE, Bridge Cheating, My Book Talk, NSA talk.

6) We hope to grade it and post it Saturday Afternoon.

Final Review-Admin

1) Final is Saturday Dec 14 1:30-3:30 in IRB 0318.

2) Can bring one sheet of notes.
Can: use both sides, type it, put what you want on it.
Can: copy a classmates, cram entire course–Bad Ideas
Can: cram THIS talk on it-Bad Idea

3) No calculators allowed.

4) Coverage: Slides/HW. Comprehensive.
5) Not on Exam: LWE, Bridge Cheating, My Book Talk, NSA talk.

6) We hope to grade it and post it Saturday Afternoon.

7) If can't take the exam tell me ASAP.

Final Review-Admin

1) Final is Saturday Dec 14 1:30-3:30 in IRB 0318.

2) Can bring one sheet of notes.
Can: use both sides, type it, put what you want on it.
Can: copy a classmates, cram entire course–Bad Ideas
Can: cram THIS talk on it-Bad Idea

3) No calculators allowed.

4) Coverage: Slides/HW. Comprehensive.
5) Not on Exam: LWE, Bridge Cheating, My Book Talk, NSA talk.

6) We hope to grade it and post it Saturday Afternoon.

7) If can't take the exam tell me ASAP.

8) Advice: Understand rather than memorize.

HW Review

December 5, 2019

Hw07, Problem 3

1. Write Rabin's Encryption algorithm. **ANS** Omitted.
2. What is the big advantage of Rabin's Encryption?

Hw07, Problem 3

1. Write Rabin's Encryption algorithm. **ANS** Omitted.
2. What is the big advantage of Rabin's Encryption?
   ANS Breaking Rabin is equivalent to factoring.

Hw07, Problem 3

1. Write Rabin's Encryption algorithm. **ANS** Omitted.
2. What is the big advantage of Rabin's Encryption?
   ANS Breaking Rabin is equivalent to factoring.
3. What is the big disadvantage of Rabin's Encryption?

Hw07, Problem 3

1. Write Rabin's Encryption algorithm. **ANS** Omitted.
2. What is the big advantage of Rabin's Encryption?
   ANS Breaking Rabin is equivalent to factoring.
3. What is the big disadvantage of Rabin's Encryption?
   ANS When Alice decodes she may get several possibilities for what the message is.

Hw07, Problem 3

1. Write Rabin's Encryption algorithm. **ANS** Omitted.
2. What is the big advantage of Rabin's Encryption?
   ANS Breaking Rabin is equivalent to factoring.
3. What is the big disadvantage of Rabin's Encryption?
   ANS When Alice decodes she may get several possibilities for what the message is.
4. Give a scenario where that disadvantage is not a problem.

Hw07, Problem 3

1. Write Rabin's Encryption algorithm. **ANS** Omitted.
2. What is the big advantage of Rabin's Encryption?
   ANS Breaking Rabin is equivalent to factoring.
3. What is the big disadvantage of Rabin's Encryption?
   ANS When Alice decodes she may get several possibilities for what the message is.
4. Give a scenario where that disadvantage is not a problem.
   ANS If Bob is sending ENGLISH texts (or something else easily recognized) then when Alice gets several decodings she can tell which one it's supposed to be.

Hw07, Problem 4

We call a set of N_1, N_2, N_3 JUSTINIAN if (1) N_1 rel prime to $N_2 N_3$, (2) N_2 rel prime to $N_1 N_3$, and (3) N_3 rel prime to $N_1 N_2$. Write Pseudocode to do the following: Given N_1, N_2, N_3 JUSTINIAN and x_1, x_2, x_3, find x such that

$$\begin{aligned} x &\equiv x_1 \pmod{N_1} \\ x &\equiv x_2 \pmod{N_2} \\ x &\equiv x_3 \pmod{N_3} \end{aligned}$$

Hw07, Problem 4

We call a set of N_1, N_2, N_3 JUSTINIAN if (1) N_1 rel prime to $N_2 N_3$, (2) N_2 rel prime to $N_1 N_3$, and (3) N_3 rel prime to $N_1 N_2$. Write Pseudocode to do the following: Given N_1, N_2, N_3 JUSTINIAN and x_1, x_2, x_3, find x such that

$$\begin{aligned} x &\equiv x_1 \pmod{N_1} \\ x &\equiv x_2 \pmod{N_2} \\ x &\equiv x_3 \pmod{N_3} \end{aligned}$$

ANS

Hw07, Problem 4

We call a set of N_1, N_2, N_3 JUSTINIAN if (1) N_1 rel prime to $N_2 N_3$, (2) N_2 rel prime to $N_1 N_3$, and (3) N_3 rel prime to $N_1 N_2$. Write Pseudocode to do the following: Given N_1, N_2, N_3 JUSTINIAN and x_1, x_2, x_3, find x such that

$$\begin{aligned} x &\equiv x_1 \pmod{N_1} \\ x &\equiv x_2 \pmod{N_2} \\ x &\equiv x_3 \pmod{N_3} \end{aligned}$$

ANS

1. Input $N_1, N_2, N_3, x_1, x_2, x_3$

Hw07, Problem 4

We call a set of N_1, N_2, N_3 JUSTINIAN if (1) N_1 rel prime to N_2N_3, (2) N_2 rel prime to N_1N_3, and (3) N_3 rel prime to N_1N_2. Write Pseudocode to do the following: Given N_1, N_2, N_3 JUSTINIAN and x_1, x_2, x_3, find x such that

$$\begin{aligned} x &\equiv x_1 \pmod{N_1} \\ x &\equiv x_2 \pmod{N_2} \\ x &\equiv x_3 \pmod{N_3} \end{aligned}$$

ANS

1. Input $N_1, N_2, N_3, x_1, x_2, x_3$
2. Find the inverse of N_1N_2 mod N_3. We call this $(N_1N_2)^{-1}$.

Hw07, Problem 4

We call a set of N_1, N_2, N_3 JUSTINIAN if (1) N_1 rel prime to N_2N_3, (2) N_2 rel prime to N_1N_3, and (3) N_3 rel prime to N_1N_2. Write Pseudocode to do the following: Given N_1, N_2, N_3 JUSTINIAN and x_1, x_2, x_3, find x such that

$$x \equiv x_1 \pmod{N_1}$$
$$x \equiv x_2 \pmod{N_2}$$
$$x \equiv x_3 \pmod{N_3}$$

ANS

1. Input $N_1, N_2, N_3, x_1, x_2, x_3$
2. Find the inverse of N_1N_2 mod N_3. We call this $(N_1N_2)^{-1}$.
3. Find the inverse of N_1N_3 mod N_2. We call this $(N_1N_3)^{-1}$.

Hw07, Problem 4

We call a set of N_1, N_2, N_3 JUSTINIAN if (1) N_1 rel prime to N_2N_3, (2) N_2 rel prime to N_1N_3, and (3) N_3 rel prime to N_1N_2. Write Pseudocode to do the following: Given N_1, N_2, N_3 JUSTINIAN and x_1, x_2, x_3, find x such that

$$\begin{aligned} x &\equiv x_1 \pmod{N_1} \\ x &\equiv x_2 \pmod{N_2} \\ x &\equiv x_3 \pmod{N_3} \end{aligned}$$

ANS

1. Input $N_1, N_2, N_3, x_1, x_2, x_3$
2. Find the inverse of N_1N_2 mod N_3. We call this $(N_1N_2)^{-1}$.
3. Find the inverse of N_1N_3 mod N_2. We call this $(N_1N_3)^{-1}$.
4. Find the inverse of N_2N_3 mod N_1. We call this $(N_2N_3)^{-1}$.

Hw07, Problem 4

We call a set of N_1, N_2, N_3 JUSTINIAN if (1) N_1 rel prime to $N_2 N_3$, (2) N_2 rel prime to $N_1 N_3$, and (3) N_3 rel prime to $N_1 N_2$. Write Pseudocode to do the following: Given N_1, N_2, N_3 JUSTINIAN and x_1, x_2, x_3, find x such that

$$\begin{aligned} x &\equiv x_1 \pmod{N_1} \\ x &\equiv x_2 \pmod{N_2} \\ x &\equiv x_3 \pmod{N_3} \end{aligned}$$

ANS

1. Input $N_1, N_2, N_3, x_1, x_2, x_3$
2. Find the inverse of $N_1 N_2$ mod N_3. We call this $(N_1 N_2)^{-1}$.
3. Find the inverse of $N_1 N_3$ mod N_2. We call this $(N_1 N_3)^{-1}$.
4. Find the inverse of $N_2 N_3$ mod N_1. We call this $(N_2 N_3)^{-1}$.
5. Output

$$x_1 (N_2 N_3)^{-1} N_2 N_3 + x_2 (N_1 N_3)^{-1} N_1 N_3 + x_3 (N_1 N_2)^{-1} N_1 N_2.$$

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969.$

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969$. $(m_1, m_2, m_3, m_4) = (8, 7, 6, 1)$.

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969$. $(m_1, m_2, m_3, m_4) = (8, 7, 6, 1)$. We generate the r's and hence the b_i's.

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969$. $(m_1, m_2, m_3, m_4) = (8, 7, 6, 1)$.
We generate the r's and hence the b_i's.
$r = 5432$.

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969$. $(m_1, m_2, m_3, m_4) = (8, 7, 6, 1)$.
We generate the r's and hence the b_i's.
$r = 5432$.
$x_1 = 5432^2 \equiv 590461 \pmod{N}$, hence $b_1 = 1$.

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969$. $(m_1, m_2, m_3, m_4) = (8, 7, 6, 1)$.
We generate the r's and hence the b_i's.
$r = 5432$.
$x_1 = 5432^2 \equiv 590461 \pmod{N}$, hence $b_1 = 1$.
$x_2 = 590461^2 \equiv 944261 \pmod{N}$, hence $b_2 = 1$.

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969$. $(m_1, m_2, m_3, m_4) = (8, 7, 6, 1)$.
We generate the r's and hence the b_i's.
$r = 5432$.
$x_1 = 5432^2 \equiv 590461 \pmod{N}$, hence $b_1 = 1$.
$x_2 = 590461^2 \equiv 944261 \pmod{N}$, hence $b_2 = 1$.
$x_3 = 944261^2 \equiv 20985 \pmod{N}$, hence $b_3 = 5$.

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969$. $(m_1, m_2, m_3, m_4) = (8, 7, 6, 1)$.
We generate the r's and hence the b_i's.
$r = 5432$.
$x_1 = 5432^2 \equiv 590461 \pmod{N}$, hence $b_1 = 1$.
$x_2 = 590461^2 \equiv 944261 \pmod{N}$, hence $b_2 = 1$.
$x_3 = 944261^2 \equiv 20985 \pmod{N}$, hence $b_3 = 5$.
$x_4 = 20985^2 \equiv 201966 \pmod{N}$, hence $b_4 = 6$.

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969$. $(m_1, m_2, m_3, m_4) = (8, 7, 6, 1)$.
We generate the r's and hence the b_i's.
$r = 5432$.
$x_1 = 5432^2 \equiv 590461 \pmod{N}$, hence $b_1 = 1$.
$x_2 = 590461^2 \equiv 944261 \pmod{N}$, hence $b_2 = 1$.
$x_3 = 944261^2 \equiv 20985 \pmod{N}$, hence $b_3 = 5$.
$x_4 = 20985^2 \equiv 201966 \pmod{N}$, hence $b_4 = 6$.
$x_5 = 201966^2 \equiv 268853 \pmod{N}$.

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969$. $(m_1, m_2, m_3, m_4) = (8, 7, 6, 1)$.
We generate the r's and hence the b_i's.
$r = 5432$.
$x_1 = 5432^2 \equiv 590461 \pmod{N}$, hence $b_1 = 1$.
$x_2 = 590461^2 \equiv 944261 \pmod{N}$, hence $b_2 = 1$.
$x_3 = 944261^2 \equiv 20985 \pmod{N}$, hence $b_3 = 5$.
$x_4 = 20985^2 \equiv 201966 \pmod{N}$, hence $b_4 = 6$.
$x_5 = 201966^2 \equiv 268853 \pmod{N}$.
Bob computes the following (all arithmetic mod 10)
$(b_1 + m_1, b_2 + m_2, b_3 + m_3, b_4 + m_4) =$
$(1 + 8, 1 + 7, 5 + 6, 6 + 1) \equiv (9, 8, 1, 7) \pmod{10}$.

Hw07, Prob 5

($\oplus$ is $+$ mod 10.) Alice and Bob are doing BG with $p = 1019$, $q = 1051$, $r = 5432$, and $m = 8761$. What does Bob send?

ANS $N = 1019 \times 1051 = 1070969$. $(m_1, m_2, m_3, m_4) = (8, 7, 6, 1)$.
We generate the r's and hence the b_i's.
$r = 5432$.
$x_1 = 5432^2 \equiv 590461 \pmod{N}$, hence $b_1 = 1$.
$x_2 = 590461^2 \equiv 944261 \pmod{N}$, hence $b_2 = 1$.
$x_3 = 944261^2 \equiv 20985 \pmod{N}$, hence $b_3 = 5$.
$x_4 = 20985^2 \equiv 201966 \pmod{N}$, hence $b_4 = 6$.
$x_5 = 201966^2 \equiv 268853 \pmod{N}$.
Bob computes the following (all arithmetic mod 10)
$(b_1 + m_1, b_2 + m_2, b_3 + m_3, b_4 + m_4) =$
$(1 + 8, 1 + 7, 5 + 6, 6 + 1) \equiv (9, 8, 1, 7) \pmod{10}$.
He then sends $((9, 8, 1, 7), 268853)$.

Hw08, Prob 2

Recall the following key exchange protocol:

Hw08, Prob 2

Recall the following key exchange protocol:

1. Alice generates rand prime p of length L, rand $S \times S$ matrix A over $\mathbb{Z}_p$. You can assume A is invertible.

Hw08, Prob 2

Recall the following key exchange protocol:

1. Alice generates rand prime p of length L, rand $S \times S$ matrix A over $\mathbb{Z}_p$. You can assume A is invertible.
2. Alice sends $(p, A, HAHA)$. All public.

Hw08, Prob 2

Recall the following key exchange protocol:

1. Alice generates rand prime p of length L, rand $S \times S$ matrix A over $\mathbb{Z}_p$. You can assume A is invertible.
2. Alice sends $(p, A, HAHA)$. All public.
3. Alice generates rand row $\vec{y} \in \mathbb{Z}_p^S$. Sends $\vec{y}A$.

Hw08, Prob 2

Recall the following key exchange protocol:

1. Alice generates rand prime p of length L, rand $S \times S$ matrix A over $\mathbb{Z}_p$. You can assume A is invertible.
2. Alice sends $(p, A, HAHA)$. All public.
3. Alice generates rand row $\vec{y} \in \mathbb{Z}_p^S$. Sends $\vec{y}A$.
4. Bob generate rand column $\vec{x} \in \mathbb{Z}_p^S$, Sends $A\vec{x}$.

Hw08, Prob 2

Recall the following key exchange protocol:

1. Alice generates rand prime p of length L, rand $S \times S$ matrix A over $\mathbb{Z}_p$. You can assume A is invertible.
2. Alice sends $(p, A, HAHA)$. All public.
3. Alice generates rand row $\vec{y} \in \mathbb{Z}_p^S$. Sends $\vec{y}A$.
4. Bob generate rand column $\vec{x} \in \mathbb{Z}_p^S$, Sends $A\vec{x}$.
5. Alice computes $\vec{y}(A\vec{x}) = \vec{y}A\vec{x}$.

Hw08, Prob 2

Recall the following key exchange protocol:

1. Alice generates rand prime p of length L, rand $S \times S$ matrix A over $\mathbb{Z}_p$. You can assume A is invertible.
2. Alice sends $(p, A, HAHA)$. All public.
3. Alice generates rand row $\vec{y} \in \mathbb{Z}_p^S$. Sends $\vec{y}A$.
4. Bob generate rand column $\vec{x} \in \mathbb{Z}_p^S$, Sends $A\vec{x}$.
5. Alice computes $\vec{y}(A\vec{x}) = \vec{y}A\vec{x}$.
6. Bob computes $(\vec{y}A)\vec{x} = \vec{y}A\vec{x}$.

Hw08, Prob 2

Recall the following key exchange protocol:

1. Alice generates rand prime p of length L, rand $S \times S$ matrix A over $\mathbb{Z}_p$. You can assume A is invertible.
2. Alice sends $(p, A, HAHA)$. All public.
3. Alice generates rand row $\vec{y} \in \mathbb{Z}_p^S$. Sends $\vec{y}A$.
4. Bob generate rand column $\vec{x} \in \mathbb{Z}_p^S$, Sends $A\vec{x}$.
5. Alice computes $\vec{y}(A\vec{x}) = \vec{y}A\vec{x}$.
6. Bob computes $(\vec{y}A)\vec{x} = \vec{y}A\vec{x}$.
7. Alice and Bob have shared secret $\vec{y}A\vec{x}$

Eve sees $(p, A, HAHA, \vec{y}A, A\vec{x})$. Help Eve recover $\vec{y}A\vec{x}$.

Hw08, Prob 2

Recall the following key exchange protocol:

1. Alice generates rand prime p of length L, rand $S \times S$ matrix A over $\mathbb{Z}_p$. You can assume A is invertible.
2. Alice sends $(p, A, HAHA)$. All public.
3. Alice generates rand row $\vec{y} \in \mathbb{Z}_p^S$. Sends $\vec{y}A$.
4. Bob generate rand column $\vec{x} \in \mathbb{Z}_p^S$, Sends $A\vec{x}$.
5. Alice computes $\vec{y}(A\vec{x}) = \vec{y}A\vec{x}$.
6. Bob computes $(\vec{y}A)\vec{x} = \vec{y}A\vec{x}$.
7. Alice and Bob have shared secret $\vec{y}A\vec{x}$

Eve sees $(p, A, HAHA, \vec{y}A, A\vec{x})$. Help Eve recover $\vec{y}A\vec{x}$.
ANS Eve computes A^{-1}, and then computes $A^{-1}A\vec{x} = \vec{x}$. Eve knows x and $\vec{y}A$ so she can compute $\vec{y}A\vec{x}$.

Motivation Behind Hw08, Prob 3

HW 08, Prob 3 was motivated by a student asking
Why do we do Diffie-Helman over $\mathbb{Z}_p$ instead of just over $\mathbb{N}$?

Motivation Behind Hw08, Prob 3

HW 08, Prob 3 was motivated by a student asking
Why do we do Diffie-Helman over $\mathbb{Z}_p$ instead of just over $\mathbb{N}$?

SO, I will go over the problem, not as asked, but to make the point of why doing DH over $\mathbb{N}$ would be a bad idea.

Hw08, Prob 3

A and B do DH over $\mathbb{N}$.

Hw08, Prob 3

A and B do DH over $\mathbb{N}$.

1. Security parameters are S, T.

Hw08, Prob 3

A and B do DH over $\mathbb{N}$.

1. Security parameters are S, T.
2. Alice picks a random $g \in \{2, \ldots, S\}$ and broadcasts g.

Hw08, Prob 3

A and B do DH over $\mathbb{N}$.

1. Security parameters are S, T.
2. Alice picks a random $g \in \{2, \ldots, S\}$ and broadcasts g.
3. Alice picks a random $a \in \{2, \ldots, T\}$ and broadcasts g^a.

Hw08, Prob 3

A and B do DH over $\mathbb{N}$.

1. Security parameters are S, T.
2. Alice picks a random $g \in \{2, \ldots, S\}$ and broadcasts g.
3. Alice picks a random $a \in \{2, \ldots, T\}$ and broadcasts g^a.
4. Bob picks a random $b \in \{2, \ldots, T\}$ and broadcasts g^b.

Hw08, Prob 3

A and B do DH over $\mathbb{N}$.

1. Security parameters are S, T.
2. Alice picks a random $g \in \{2, \ldots, S\}$ and broadcasts g.
3. Alice picks a random $a \in \{2, \ldots, T\}$ and broadcasts g^a.
4. Bob picks a random $b \in \{2, \ldots, T\}$ and broadcasts g^b.
5. Alice computes $(g^b)^a = g^{ab}$.

Hw08, Prob 3

A and B do DH over $\mathbb{N}$.

1. Security parameters are S, T.
2. Alice picks a random $g \in \{2, \ldots, S\}$ and broadcasts g.
3. Alice picks a random $a \in \{2, \ldots, T\}$ and broadcasts g^a.
4. Bob picks a random $b \in \{2, \ldots, T\}$ and broadcasts g^b.
5. Alice computes $(g^b)^a = g^{ab}$.
6. Bob computes $(g^a)^b = g^{ab}$.

Hw08, Prob 3

A and B do DH over $\mathbb{N}$.

1. Security parameters are S, T.
2. Alice picks a random $g \in \{2, \ldots, S\}$ and broadcasts g.
3. Alice picks a random $a \in \{2, \ldots, T\}$ and broadcasts g^a.
4. Bob picks a random $b \in \{2, \ldots, T\}$ and broadcasts g^b.
5. Alice computes $(g^b)^a = g^{ab}$.
6. Bob computes $(g^a)^b = g^{ab}$.
7. The shared secret key is g^{ab}.

We Look at DIFF Problems than the HW looked at
What are the PROS and CONS of doing DH over $\mathbb{N}$?

Hw08, Prob 3: PROS

Hw08, Prob 3: PROS

PROS

Hw08, Prob 3: PROS

PROS

PRO: Can still use repeated squaring. So if count each operation as one step, still fast.

Hw08, Prob 3: PROS

PROS

PRO: Can still use repeated squaring. So if count each operation as one step, still fast.

CAVEAT: Numbers could get big. If they do then the assumption of one-operation takes one-step is no longer true.

Hw08, Prob 3: PROS

PROS

PRO: Can still use repeated squaring. So if count each operation as one step, still fast.

CAVEAT: Numbers could get big. If they do then the assumption of one-operation takes one-step is no longer true.

EXAMPLE:

1. If all of the numbers are ≤ 1000 then addition, sub, mult, div, all take 1 step. Not really 1 but a small number, say $O(1)$.
2. If you need to square

   $$23456789009876545678907709877666911001133399393993333991 2$$

   That is looking like A LOT of steps.

Hw08, Prob 3: How Fast is Mult of Big Numbers?

KNOWN:

Hw08, Prob 3: How Fast is Mult of Big Numbers?

KNOWN:

1. There is an algorithm to multiply 2 L-bit numbers in time $O(L^2)$. You did this in High School.

Hw08, Prob 3: How Fast is Mult of Big Numbers?

KNOWN:

1. There is an algorithm to multiply 2 L-bit numbers in time $O(L^2)$. You did this in High School.
2. There is an algorithm to multiply 2 L-bit numbers in time $O(L^{1.585})$. This you may have learned in CMSC 351.

Hw08, Prob 3: How Fast is Mult of Big Numbers?

KNOWN:

1. There is an algorithm to multiply 2 L-bit numbers in time $O(L^2)$. You did this in High School.
2. There is an algorithm to multiply 2 L-bit numbers in time $O(L^{1.585})$. This you may have learned in CMSC 351.
3. There is an algorithm to multiply 2 L-bit numbers in time $O(L \log L \log \log L)$. This is difficult.

Hw08, Prob 3: How Fast is Mult of Big Numbers?

KNOWN:

1. There is an algorithm to multiply 2 L-bit numbers in time $O(L^2)$. You did this in High School.
2. There is an algorithm to multiply 2 L-bit numbers in time $O(L^{1.585})$. This you may have learned in CMSC 351.
3. There is an algorithm to multiply 2 L-bit numbers in time $O(L \log L \log\log L)$. This is difficult.
4. Better algorithms are known, but not much better, and not usable.

Point If L is large then you can no longer regard mult of 2 n-bit numbers as $O(1)$ time.

Hw08, Prob 3: CONS

Hw08, Prob 3: CONS

CON: With big numbers, might take too much time or space.

Hw08, Prob 3: CONS

CON: With big numbers, might take too much time or space.

BIGGEST CON: Contrast: Discrete Log seems hard over $\mathbb{Z}_p$ since $x \rightarrow g^x$ is random-looking. But Log over $\mathbb{N}$ is very easy since log is monotone. Binary Search works very well. And there are faster ways (e.g., Taylor series)

Hw09, Prob 2: Set Up

Want to factor 81072007 with QS

Hw09, Prob 2: Set Up

Want to factor 81072007 with QS

- Note that $\lceil \sqrt{81072007} \rceil = 9004$.

Hw09, Prob 2: Set Up

Want to factor 81072007 with QS

- Note that $\lceil \sqrt{81072007} \rceil = 9004$.
- Will factor $(9004 + x)^2$ instead of B-factor.

Hw09, Prob 2: Set Up

Want to factor 81072007 with QS

- Note that $\lceil \sqrt{81072007} \rceil = 9004$.
- Will factor $(9004 + x)^2$ instead of B-factor.
- We only use x such that $(9004 + x)^2 - 81072007 \equiv 0 \pmod{6}$. This way we know that 2 and 3 both divide $(9004 + x)^2$ so it has some factors.

Hw09, Prob 2: Set Up

Want to factor 81072007 with QS

- Note that $\lceil\sqrt{81072007}\rceil = 9004$.
- Will factor $(9004+x)^2$ instead of B-factor.
- We only use x such that $(9004+x)^2 - 81072007 \equiv 0 \pmod{6}$. This way we know that 2 and 3 both divide $(9004+x)^2$ so it has some factors.

The problem had three parts which culminate in obtaining a factor.

Hw09, Prob 2: Set Up

Want to factor 81072007 with QS

- Note that $\lceil \sqrt{81072007} \rceil = 9004$.
- Will factor $(9004 + x)^2$ instead of B-factor.
- We only use x such that $(9004 + x)^2 - 81072007 \equiv 0 \pmod 6$. This way we know that 2 and 3 both divide $(9004 + x)^2$ so it has some factors.

The problem had three parts which culminate in obtaining a factor.

We do each part on a diff slide.

Find which x to Use

Find $X \subseteq \{0, 1, 2, 3, 4, 5\}$ such that:

$$((9004 + x)^2 - 81072007 \equiv 0 \pmod 6) IFF (x \bmod 6 \in X).$$

Find which x to Use

Find $X \subseteq \{0,1,2,3,4,5\}$ such that:

$$((9004+x)^2 - 81072007 \equiv 0 \pmod 6) IFF (x \bmod 6 \in X).$$

ANS
$(9004+x)^2 - 81072007 \equiv 0 \pmod 6$

Find which x to Use

Find $X \subseteq \{0,1,2,3,4,5\}$ such that:

$$((9004 + x)^2 - 81072007 \equiv 0 \pmod 6) IFF (x \bmod 6 \in X).$$

ANS

$(9004 + x)^2 - 81072007 \equiv 0 \pmod 6$

Mod down:

Find which x to Use

Find $X \subseteq \{0, 1, 2, 3, 4, 5\}$ such that:

$$((9004 + x)^2 - 81072007 \equiv 0 \pmod 6) IFF (x \bmod 6 \in X).$$

ANS

$(9004 + x)^2 - 81072007 \equiv 0 \pmod 6$

Mod down:

$(4 + x)^2 - 1 \equiv 0 \pmod 6$

Find which x to Use

Find $X \subseteq \{0,1,2,3,4,5\}$ such that:

$$((9004 + x)^2 - 81072007 \equiv 0 \pmod 6) IFF (x \bmod 6 \in X).$$

ANS

$(9004 + x)^2 - 81072007 \equiv 0 \pmod 6$

Mod down:

$(4 + x)^2 - 1 \equiv 0 \pmod 6$

Need to know when $(x + 4)^2 \equiv 1 \pmod 6$.

Try $0, 1, 2, 3, 4, 5$ and find $X = \{1, 3\}$.

Factor $(9004 + x)^2 - 81072007$

For $x \geq 0$ with $x \bmod 6 \in X$, factor $(9004 + x)^2 - 81072007$ until have what is needed for QS.

Factor $(9004 + x)^2 - 81072007$

For $x \geq 0$ with $x \bmod 6 \in X$, factor $(9004 + x)^2 - 81072007$ until have what is needed for QS.

x	$(9004 + x)^2$	$(9004 + x)^2 - 81072007$		factored
1	9005^2	$\equiv 18018$	$=$	$2 \times 3^2 \times 7 \times 11 \times 13$
3	9007^2	$\equiv 54042$	$=$	$2 \times 3 \times 9007$
7	9011^2	$\equiv 126114$	$=$	$2 \times 3 \times 21019$
9	9013^2	$\equiv 162162$	$=$	$2 \times 3^4 \times 7 \times 11 \times 13$

Factor $(9004+x)^2 - 81072007$

For $x \geq 0$ with $x \bmod 6 \in X$, factor $(9004+x)^2 - 81072007$ until have what is needed for QS.

x	$(9004+x)^2$	$(9004+x)^2 - 81072007$		factored
1	9005^2	$\equiv 18018$	$=$	$2 \times 3^2 \times 7 \times 11 \times 13$
3	9007^2	$\equiv 54042$	$=$	$2 \times 3 \times 9007$
7	9011^2	$\equiv 126114$	$=$	$2 \times 3 \times 21019$
9	9013^2	$\equiv 162162$	$=$	$2 \times 3^4 \times 7 \times 11 \times 13$

AH-HA! - we can mult first and fourth row

$$(9005 \times 9013)^2 \equiv 2^2 \times 3^6 \times 7^2 \times 11^2 \times 13^2$$

Factor $(9004 + x)^2 - 81072007$

For $x \geq 0$ with $x \bmod 6 \in X$, factor $(9004 + x)^2 - 81072007$ until have what is needed for QS.

x	$(9004 + x)^2$	$(9004 + x)^2 - 81072007$		factored
1	9005^2	$\equiv 18018$	$=$	$2 \times 3^2 \times 7 \times 11 \times 13$
3	9007^2	$\equiv 54042$	$=$	$2 \times 3 \times 9007$
7	9011^2	$\equiv 126114$	$=$	$2 \times 3 \times 21019$
9	9013^2	$\equiv 162162$	$=$	$2 \times 3^4 \times 7 \times 11 \times 13$

AH-HA! - we can mult first and fourth row

$$(9005 \times 9013)^2 \equiv 2^2 \times 3^6 \times 7^2 \times 11^2 \times 13^2$$

$$(9005 \times 9013)^2 \equiv (2 \times 3^3 \times 7 \times 11 \times 13)^2$$

Use Last Part to Factor

$$(9005 \times 9013)^2 \equiv (2 \times 3^3 \times 7 \times 11 \times 13)^2$$

Use Last Part to Factor

$$(9005 \times 9013)^2 \equiv (2 \times 3^3 \times 7 \times 11 \times 13)^2$$

$$81162065^2 \equiv 54054^2 \pmod{81072007}$$

Use Last Part to Factor

$$(9005 \times 9013)^2 \equiv (2 \times 3^3 \times 7 \times 11 \times 13)^2$$

$$81162065^2 \equiv 54054^2 \pmod{81072007}$$

Mod down:

$$90058^2 \equiv 54054^2$$

Use Last Part to Factor

$$(9005 \times 9013)^2 \equiv (2 \times 3^3 \times 7 \times 11 \times 13)^2$$

$$81162065^2 \equiv 54054^2 \pmod{81072007}$$

Mod down:

$$90058^2 \equiv 54054^2$$

$$(90058 - 54054)(90058 + 54054) \equiv 0$$

Use Last Part to Factor

$$(9005 \times 9013)^2 \equiv (2 \times 3^3 \times 7 \times 11 \times 13)^2$$

$$81162065^2 \equiv 54054^2 \pmod{81072007}$$

Mod down:

$$90058^2 \equiv 54054^2$$

$$(90058 - 54054)(90058 + 54054) \equiv 0$$

$$36004 \times 144112 \equiv 0$$

Use Last Part to Factor

$$(9005 \times 9013)^2 \equiv (2 \times 3^3 \times 7 \times 11 \times 13)^2$$

$$81162065^2 \equiv 54054^2 \pmod{81072007}$$

Mod down:

$$90058^2 \equiv 54054^2$$

$$(90058 - 54054)(90058 + 54054) \equiv 0$$

$$36004 \times 144112 \equiv 0$$

$GCD(36004, 81072007) = 9001$ is a factor. Done!

Hw09, Prob 2: Commentary

We had:

x	$(9004+x)^2$	$(9004+x)^2 - 81072007$		factored
1	9005^2	$\equiv 18018$	$=$	$2 \times 3^2 \times 7 \times 11 \times 13$
3	9007^2	$\equiv 54042$	$=$	$2 \times 3 \times 9007$
7	9011^2	$\equiv 126114$	$=$	$2 \times 3 \times 21019$
9	9013^2	$\equiv 162162$	$=$	$2 \times 3^4 \times 7 \times 11 \times 13$

and we said AH HA: The First and Fourth Column.

Hw09, Prob 2: Commentary

We had:

x	$(9004+x)^2$	$(9004+x)^2 - 81072007$		factored
1	9005^2	$\equiv 18018$	$=$	$2 \times 3^2 \times 7 \times 11 \times 13$
3	9007^2	$\equiv 54042$	$=$	$2 \times 3 \times 9007$
7	9011^2	$\equiv 126114$	$=$	$2 \times 3 \times 21019$
9	9013^2	$\equiv 162162$	$=$	$2 \times 3^4 \times 7 \times 11 \times 13$

and we said AH HA: The First and Fourth Column.

The first and fourth both have 2,3,7,11,13 as primes. Having same primes NOT always the case. The following could happen:

1	$2^2 \times 3 \times 7 \times 11$
2	$3 \times 7^2 \times 11$
3	$7^3 \times 11^8 \times 13^2$

Mult all three to get

$$2^2 \times 3^2 \times 7^6 \times 11^{10} \times 13^2 = (2 \times 3 \times 7^3 \times 11^5)^2$$

Hw09, Prob 3: Setup

Eve wants to factor $G = 139,323,391$ (a product of two primes) using the method Golomb used to factor the Jevons number.

This problem will guide you through it.

Hw09, Prob 3: Setup

Eve wants to factor $G = 139,323,391$ (a product of two primes) using the method Golomb used to factor the Jevons number.

This problem will guide you through it.

Throughout this problem x, y are such that $G = x^2 - y^2$. During this problem we reduce the number of options for (x, y).

Hw09, Prob 3: Setup

Eve wants to factor $G = 139,323,391$ (a product of two primes) using the method Golomb used to factor the Jevons number.

This problem will guide you through it.

Throughout this problem x, y are such that $G = x^2 - y^2$. During this problem we reduce the number of options for (x, y).

Each part is on its own slide.

Find d

Find a $0 \leq d \leq 99$ such that the following holds:

$$y^2 \equiv x^2 + d \pmod{100}$$

Find d

Find a $0 \leq d \leq 99$ such that the following holds:

$$y^2 \equiv x^2 + d \pmod{100}$$

ANS

$$G = x^2 - y^2$$

Find d

Find a $0 \leq d \leq 99$ such that the following holds:

$$y^2 \equiv x^2 + d \pmod{100}$$

ANS

$$G = x^2 - y^2$$

$$91 \equiv x^2 - y^2 \pmod{100}$$

Find d

Find a $0 \leq d \leq 99$ such that the following holds:

$$y^2 \equiv x^2 + d \pmod{100}$$

ANS

$$G = x^2 - y^2$$

$$91 \equiv x^2 - y^2 \pmod{100}$$

$$y^2 \equiv x^2 + 9 \pmod{100}$$

Find d

Find a $0 \leq d \leq 99$ such that the following holds:

$$y^2 \equiv x^2 + d \pmod{100}$$

ANS

$$G = x^2 - y^2$$

$$91 \equiv x^2 - y^2 \pmod{100}$$

$$y^2 \equiv x^2 + 9 \pmod{100}$$

$$d = 9.$$

Possible (x, y)

List all possibilities for $(x^2 \bmod 100, y^2 \bmod 100)$.

Possible (x, y)

List all possibilities for $(x^2 \bmod 100, y^2 \bmod 100)$.

ANS

The following is the set of all squares mod 100

$$\{0, 1, 4, 9, 16, 21, 24, 25, 29, 36, 41, 44, 49\} \cup$$

$$\{56, 61, 64, 69, 76, 81, 84, 89, 96\}$$

Possible (x, y)

List all possibilities for $(x^2 \bmod 100, y^2 \bmod 100)$.
ANS
The following is the set of all squares mod 100

$$\{0, 1, 4, 9, 16, 21, 24, 25, 29, 36, 41, 44, 49\} \cup$$

$$\{56, 61, 64, 69, 76, 81, 84, 89, 96\}$$

Need all pairs that differ by 9 mod 100:

Possible (x, y)

List all possibilities for $(x^2 \bmod 100, y^2 \bmod 100)$.

ANS

The following is the set of all squares mod 100

$$\{0, 1, 4, 9, 16, 21, 24, 25, 29, 36, 41, 44, 49\} \cup$$

$$\{56, 61, 64, 69, 76, 81, 84, 89, 96\}$$

Need all pairs that differ by 9 mod 100:

$$\{(0, 9), (16, 25)\}$$

Narrow Down Search for x

Find all $x \pmod{100}$ such that $x^2 \equiv 0 \pmod{100}$ OR $x^2 \equiv 16 \pmod{100}$. Put the union of the two sets into numeric order.

Note that at the end you will have a small set A such that

$$x \bmod 100 \in A.$$

Narrow Down Search for x

Find all $x \pmod{100}$ such that $x^2 \equiv 0 \pmod{100}$ OR $x^2 \equiv 16 \pmod{100}$. Put the union of the two sets into numeric order.

Note that at the end you will have a small set A such that

$$x \bmod 100 \in A.$$

ANS

$x^2 \equiv 0 \pmod{100}$ has solutions

$$\{0, 10, 20, 30, 40, 50, 60, 70, 80, 90\}$$

Narrow Down Search for x

Find all $x \pmod{100}$ such that $x^2 \equiv 0 \pmod{100}$ OR $x^2 \equiv 16 \pmod{100}$. Put the union of the two sets into numeric order.

Note that at the end you will have a small set A such that

$$x \bmod 100 \in A.$$

ANS
$x^2 \equiv 0 \pmod{100}$ has solutions

$$\{0, 10, 20, 30, 40, 50, 60, 70, 80, 90\}$$

$x^2 \equiv 16 \pmod{100}$ has solutions

$$\{4, 46, 54, 96\}$$

Narrow Down Search for x

Find all $x \pmod{100}$ such that $x^2 \equiv 0 \pmod{100}$ OR $x^2 \equiv 16 \pmod{100}$. Put the union of the two sets into numeric order.

Note that at the end you will have a small set A such that

$$x \bmod 100 \in A.$$

ANS

$x^2 \equiv 0 \pmod{100}$ has solutions

$$\{0, 10, 20, 30, 40, 50, 60, 70, 80, 90\}$$

$x^2 \equiv 16 \pmod{100}$ has solutions

$$\{4, 46, 54, 96\}$$

Putting it together we get

$$\{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$$

Bound x

Show that $x \geq \sqrt{G}$

ANS

$G = x^2 - y^2$ so

Bound x

Show that $x \geq \sqrt{G}$

ANS

$G = x^2 - y^2$ so

$$x^2 = G + y^2$$

pause

$$x = \sqrt{G + y^2} \geq \sqrt{G}.$$

Factor G

Complete the algorithm and factor G.

ANS

$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$

Factor G

Complete the algorithm and factor G.

ANS

$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$

$x \geq \sqrt{G} = 11803$

Factor G

Complete the algorithm and factor G.

ANS

$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$

$x \geq \sqrt{G} = 11803$

$y = \sqrt{x^2 - 139323391}$

Factor G

Complete the algorithm and factor G.

ANS

$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$

$x \geq \sqrt{G} = 11803$

$y = \sqrt{x^2 - 139323391}$

Table that tries out all $x \geq 11803$

Factor G

Complete the algorithm and factor G.

ANS

$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$

$x \geq \sqrt{G} = 11803$

$y = \sqrt{x^2 - 139323391}$

Table that tries out all $x \geq 11803$

x	$y = (x^2 - 139323391)^{1/2}$
11804	105

Factor G

Complete the algorithm and factor G.

ANS

$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$

$x \geq \sqrt{G} = 11803$

$y = \sqrt{x^2 - 139323391}$

Table that tries out all $x \geq 11803$

x	$y = (x^2 - 139323391)^{1/2}$
11804	105

WOW- that table ended very fast! $x = 11804$, $y = 105$

Factor G

Complete the algorithm and factor G.

ANS

$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$

$x \geq \sqrt{G} = 11803$

$y = \sqrt{x^2 - 139323391}$

Table that tries out all $x \geq 11803$

x	$y = (x^2 - 139323391)^{1/2}$
11804	105

WOW- that table ended very fast! $x = 11804$, $y = 105$

$x^2 - y^2 = 139323391$

Factor G

Complete the algorithm and factor G.

ANS

$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$

$x \geq \sqrt{G} = 11803$

$y = \sqrt{x^2 - 139323391}$

Table that tries out all $x \geq 11803$

x	$y = (x^2 - 139323391)^{1/2}$
11804	105

WOW- that table ended very fast! $x = 11804$, $y = 105$

$x^2 - y^2 = 139323391$

$(x + y)(x - y) = 139323391$

Factor G

Complete the algorithm and factor G.

ANS

$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$

$x \geq \sqrt{G} = 11803$

$y = \sqrt{x^2 - 139323391}$

Table that tries out all $x \geq 11803$

x	$y = (x^2 - 139323391)^{1/2}$
11804	105

WOW- that table ended very fast! $x = 11804$, $y = 105$

$x^2 - y^2 = 139323391$

$(x + y)(x - y) = 139323391$

$$(11804 + 105)(11804 - 105) = 139323391$$

Factor G

Complete the algorithm and factor G.

ANS

$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$

$x \ge \sqrt{G} = 11803$

$y = \sqrt{x^2 - 139323391}$

Table that tries out all $x \ge 11803$

x	$y = (x^2 - 139323391)^{1/2}$
11804	105

WOW- that table ended very fast! $x = 11804$, $y = 105$

$x^2 - y^2 = 139323391$

$(x + y)(x - y) = 139323391$

$$(11804 + 105)(11804 - 105) = 139323391$$

$$11909 \times 11699 = 139323391$$

Similar to Quad Sieve?

Want to factor G.

Similar to Quad Sieve?

Want to factor G.

Golumb's algorithm looks for x, y such that $x^2 - y^2 = G$.
The key is to cut down on the pairs (x, y) to check.

Similar to Quad Sieve?

Want to factor G.

Golumb's algorithm looks for x, y such that $x^2 - y^2 = G$.
The key is to cut down on the pairs (x, y) to check.

Quad Sieve Alg looks for x, y such that $x^2 - y^2 \equiv 0 \pmod{G}$.
They key is to use Quad Sieve Method (B-factoring) to create x, y.

Hw10, Part 1

READ MIDTERM SOLUTIONS

Hw10, Prob3, The Problem

Take the first 20 numbers y of QS and compute

$$\lceil \log_{10}(y) \rceil - \sum_{p \text{ div } y} \lceil \log_{10}(p) \rceil .$$

Hw10, Prob3, The Problem

Take the first 20 numbers y of QS and compute

$$\lceil \log_{10}(y) \rceil - \sum_{p \text{ div } y} \lceil \log_{10}(p) \rceil .$$

For each one see if it IS B-factorable.

Hw10, Prob3, The Problem

Take the first 20 numbers y of QS and compute

$$\lceil \log_{10}(y) \rceil - \sum_{p \text{ div } y} \lceil \log_{10}(p) \rceil .$$

For each one see if it IS B-factorable.

Determine what big and small should be.

Hw10, Prob 3, The Answer

1. $(7284+1)^2 \equiv 26328$. primes: 2, 3. Diff: $5-1-1=3$.
   $(7284+1)^2 \equiv 26328 = 2^3 \times 3 \times 1097$. NOT B-fact.
2. $(7284+4)^2 \equiv 70047$. primes: 3, 43. Diff: $5-1-2=2$.
   $(7284+4)^2 \equiv 70047 = 3^2 \times 43 \times 181$. NOT B-fact.
3. $(7284+5)^2 \equiv 84624$. primes: 2,3,41,43. Diff:
   $5-1-1-2-2=-1$.
   $(7284+5)^2 \equiv 84624 = 2^4 \times 3 \times 41 \times 43$. IS B-fact.
4. $(7284+7)^2 \equiv 113784$. primes: 2,3,11. Diff: $6-1-1-2=2$.
   $(7284+7)^2 \equiv 113784 = 2^3 \times 3 \times 11 \times 431$. NOT B-fact.
5. $(7284+8)^2 \equiv 128367$. primes: 3,17. Diff: $6-1-2=3$.
   $(7284+8)^2 \equiv 128367 = 3^2 \times 17 \times 839$. NOT B-fact
6. $(7284+10)^2 \equiv 157539$. primes: 3,17. Diff: $6-1-2=3$.
   $(7284+10)^2 \equiv 157539 = 3 \times 17 \times 3089$. NOT B-fact

Hw10, Prob 3, Answer, Continued

1. $(7284+11)^2 \equiv 172128$. primes: 2,3,11. Diff: $6-1-1-2=2$.
   $(7284+11)^2 \equiv 172128 = 2^5 \times 3 \times 11 \times 163$. NOT B-fact
2. $(7284+13)^2 \equiv 201312$. primes: 2,3. Diff: $6-1-1=4$.
   $(7284+13)^2 \equiv 201312 = 2^5 \times 3^3 \times 233$. NOT B-fact
3. $(7284+17)^2 \equiv 259704$. primes: 2,3. Diff: $6-1-1=4$.
   $(7284+17)^2 \equiv 259704 = 2^3 \times 3^2 \times 3607$. NOT B-fact
4. $(7284+19)^2 \equiv 288912$. primes: 2,3,13. Diff: $6-1-1-2=2$.
   $(7284+19)^2 \equiv 288912 = 2^4 \times 3 \times 13 \times 463$. NOT B-fact

We can take $s=-1$. $s=0$ and $s=1$ also work and are probably better.

Hw11, Prob 1

READ MIDTERM SOLUTIONS

Hw11, Prob 2: Setup

Zelda wants to do $(7, 14)$ information-theoretic secret sharing. The players are $A_1, \ldots, A_{14}$. The secret string is 1001.

Hw11, Prob 2a

Zelda wants to use the random string method. How many strings does A_1 get? How long are the strings A_1 gets?

ANS

A_1 will get a string for EVERY 7-sized set she is a member of. So that will be

$$\binom{13}{6} = \frac{13!}{6!7!} = \frac{13 \times 12 \times 11 \times 10 \times 9 \times 8}{6 \times 5 \times 4 \times 3 \times 2}$$

The 12 cancels with the 3×4. The 10 cancels the 2×5. So we end up with:

$$\frac{13 \times 11 \times 9 \times 8}{6} = 13 \times 11 \times 3 \times 4 = 1716.$$

So there are 1716 strings. Each string is the same length as the secret, so that is length 4.

Hw11, Prob 2b

Zelda wants to use the polynomial method. What is the smallest prime Zelda can use? What is the degree of the polynomial that Zelda uses? How many strings does A_1 get? How long are they?

ANS

We need a prime p such that $2^4 < p$, so we take 17. The degree is 6 since 7 points determine a 6th degree polynomial. A_1 gets just one string. The string is in $\mathbb{Z}_{17}$ padded out to length 4.

Hw11, Prob 3: The Problem

DESCRIBE the random-string $(3,9)$ secret sharing scheme. You must describe both what Zelda gives out, and how any three people can determine the secret.

How long are the string A_1 gets? How many strings does A_1 get?

DO AN EXAMPLE (we omit this in the solution).

Hw11, Prob 3: The Answer

ANS

We call the people $A_1, \ldots, A_9$. We give the $(3, 9)$ secret sharing method via random strings.

1. Zelda has secret s.
2. For every $1 \le i < j < k \le 9$, Zelda generates two random strings: $r_{i,j,k,i}$, $r_{i,j,k,j}$, We now visit every triple and say what Zelda gives them. All of the players will be visited many times. How many? $\binom{8}{2}$ which is the number of triples they are in. Let $1 \le i < j < k \le 9$.
   - Give A_i the string $(i, j, k, r_{i,j,k,i})$
   - Give A_j the string $(i, j, k, r_{i,j,k,j})$
   - Give A_k the string $(i, j, k, r_{i,j,k,i} \oplus r_{i,j,k,j} \oplus s))$
3. If A_i, A_j, A_k get together they will compute

$$r_{i,j,k,i} \oplus r_{i,j,k,j} \oplus (r_{i,j,k,i} \oplus r_{i,j,k,j} \oplus s) = s$$

Hw11, Prob 3: The Answer, Continued

A_1 gets strings of length n, the same size as the secret.

A_1 gets $\binom{8}{2} = 28$ strings.

Hw11, Prob 4: The Problem

DESCRIBE the polynomial $(4, 7)$ secret sharing scheme. You must describe both what Zelda gives out, and how any four people can determine the secret.

How many strings does each person get?

DO AN EXAMPLE of your method. (We omit this in the solution.)

Hw11, Prob 4: The Answer

1. Zelda has secret s.
2. Zelda finds a prime p such that $p > 2^{|s|}$.
   Zelda generates random $r_3, r_2, r_1 \in \{0, \ldots, p-1\}$.
   Zelda forms polynomial

   $$p(x) = r_3x^3 + r_2x^2 + r_1x + s$$

   (s was a string of 0's and 1's. We now view it as a number written in binary)
3. For all $1 \leq i \leq 7$, give A_i the number $p(i) \pmod{p}$.
4. If any four get together they have four points on a cubic. Hence they can recover the entire cubic, and hence the constant term which is the secret.

Hw11, Prob 4: The Answer, Continued

Everyone gets a string of length n, the length of the secret.

Everyone gets just one such string.

Hw12, Prob 1

READ MIDTERM SOLUTIONS

Hw12, Prob 2: Setup

Zelda does (3,5) secret sharing. The secret is of length 2, so they use the prime 5. Zelda gives out the following numbers:
A_1 gets 3,
A_2 gets 3,
A_3 gets 3,
A_4 gets 3,
A_5 gets 3.
(You prob think the secret is 3. You are correct.)

Hw12, Prob 2a: The Problem

1. A_1 and A_2 get together. Show that for $c = 0, 1, 2$, there is a quadratic polynomial over $\mathbb{Z}_5$ where ALL of the following hold:
   1.1 $f(1) = 3$
   1.2 $f(2) = 3$
   1.3 The constant term is c (which is equivalent to $f(0) = c$).

   (NOTE: it's also true for $c = 3, 4$ but I want to spare you the work. This is important because, if you did the problem with $c = 0, 1, 2, 3, 4$ you would show that A_1 and A_2 have learned NOTHING since all secrets are still possible.) **Show your work.**

Hw12, Prob 2a: The Answer

ALL $\equiv$ are mod 5.
$c = 0$: $f(x) \equiv r_2 x^2 + r_1 x + 0$. Need r_1, r_2 so that $f(1) \equiv 3$ and $f(2) \equiv 3$.
$f(1) = 3$: $r_2 + r_1 + 0 \equiv 3$, so $r_2 + r_1 \equiv 3$.
$f(2) = 3$: $4r_2 + 2r_1 + 0 \equiv 3$, so $4r_2 + 2r_1 \equiv 3$.
Algebra shows $r_2 = 1$ and $r_1 = 2$, so $f(x) \equiv x^2 + 2x$.

$c = 1$: Omitted, similar.
$c = 2$: Omitted, similar.

Prob 12, Prob 2b

Problem: What is the secret.
Answer: ALL $\equiv$ are mod 5.
$f(x) \equiv r_2x^2 + r_1x + s$
$f(1) \equiv 3$ so $r_2 + r_1 + s \equiv 3$
$f(2) \equiv 3$ so $4r_2 + 2r_1 + s \equiv 3$
$f(3) \equiv 3$ so $9r_2 + 3r_1 + s \equiv 3$, so $4r_2 + 3r_1 + s \equiv 3$.
From these can deduce $s = 3$.

Hw12, Prob 3: The Problem

Show that there is NO way to do (t, m) Verifiable Secret Sharing in a way that is information-theoretic secure.

WARNING: The scheme I showed in class for VSS was comp-secure. This has NO bearing on our problem. Just because there IS a comp-secure scheme does not mean that there is not an info-secure scheme. DO NOT MAKE THIS MISTAKE!!!!!!!!

Hw12, Prob 3: The Answer

Assume that there is a (t, m)-VSS scheme. We show that if the players have unlimited computational power then $t-1$ can crack the secret. (In fact, 1 can crack the secret but we leave that for you to figure out.)

$A_1, \ldots, A_{t-1}$ get together. They reveal their shares $s_1, \ldots, s_{t-1}$. They can find the share of A_t as follows:

They know the share is of string in $\{0,1\}^*$. Let $\{0,1\}^*$ be, in lex order, $u_1, u_2, u_3, \ldots$.

$A_1, \ldots, A_{t-1}$ try to verify that A_t's share is u_1. If they fail they try to verify u_2. Etc. Eventually they will find the share and verify it. They then have A_t's share so can crack the secret.

Hw12, Prob 4

Alice, Bob, and Carol have cards similar to those used in the Alice-Bob-Cards-Dating lecture. (e.g., hearts, spades, uparrows, downarrows, clear, opaque, pez dispencers). Alice has a bit a, Bob has a bit b, Carol has a bit c. They want to compute $a \wedge b \wedge c$ such that

1. At the end they ALL know $a \wedge b \wedge c$.
2. At the end Alice only knows a or course, and $a \wedge b \wedge c$, and whatever can be deduced from these. So
   2.1 If $a = 0$ and $a \wedge b \wedge c = 0$ then Alice knows nothing about b, c.
   2.2 If $a = 0$ and $a \wedge b \wedge c = 1$ then THIS CANNOT HAPPEN.
   2.3 If $a = 1$ and $a \wedge b \wedge c = 0$ then Alice knows that $b \wedge c = 0$, so at least one of b, c is 1.
   2.4 If $a = 1$ and $a \wedge b \wedge c = 1$ then Alice knows that $b \wedge c = 1$, so $b = c = 1$.
3. Similar for Bob and Carol.

Hw12, Prob 4: ANSWER

We give one answer. There are others.

1. Alice, Bob, and Carol each have two cards. One is clear, one is opaque.
2. There is a box with three slots in it for three cards. A light can be shined into the side of the box and will come out the other side if all three cards are clear.
3. Alice puts in a clear card if $a = 1$ and an opaque card if $a = 0$.
4. Bob puts in a clear card if $b = 1$ and an opaque card if $b = 0$.
5. Carol puts in a clear card if $c = 1$ and an opaque card if $c = 0$.

If $a = b = c = 1$ then the light shines through and the answer is 1. If ANY of them are 0 then the light DOES NOT shine through. If $a = 1$ then Alice will have NO IDEA what b or c is.