BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Other Topics I Could Have Covered

Other Classical

Other Classical

1. Playfair Cipher. This is a nice 2-sub cipher.

Other Classical

1. Playfair Cipher. This is a nice 2-sub cipher.
   PRO- Like Matrix, its 2-sub but in a nice way

Other Classical

1. Playfair Cipher. This is a nice 2-sub cipher.
   PRO- Like Matrix, its 2-sub but in a nice way
   CON- Nothing in it that points to the future or to a lesson-learned.

Other Classical

1. Playfair Cipher. This is a nice 2-sub cipher.
   PRO- Like Matrix, its 2-sub but in a nice way
   CON- Nothing in it that points to the future or to a lesson-learned.
2. Enigma Cipher used by Germany in WW II and broken by Britain lead by Alan Turing.

Other Classical

1. Playfair Cipher. This is a nice 2-sub cipher.
   PRO- Like Matrix, its 2-sub but in a nice way
   CON- Nothing in it that points to the future or to a lesson-learned.
2. Enigma Cipher used by Germany in WW II and broken by Britain lead by Alan Turing.
   PRO This is an extreme version of Vigenere and there are some interesting things about how it was cracked.

Other Classical

1. Playfair Cipher. This is a nice 2-sub cipher.
   PRO- Like Matrix, its 2-sub but in a nice way
   CON- Nothing in it that points to the future or to a lesson-learned.
2. Enigma Cipher used by Germany in WW II and broken by Britain lead by Alan Turing.
   PRO This is an extreme version of Vigenere and there are some interesting things about how it was cracked.
   PRO Brings up Alan Turing and interesting history and social history—and diversity issues.

Other Classical

1. Playfair Cipher. This is a nice 2-sub cipher.
   PRO- Like Matrix, its 2-sub but in a nice way
   CON- Nothing in it that points to the future or to a lesson-learned.
2. Enigma Cipher used by Germany in WW II and broken by Britain lead by Alan Turing.
   PRO This is an extreme version of Vigenere and there are some interesting things about how it was cracked.
   PRO Brings up Alan Turing and interesting history and social history—and diversity issues.
   CON Details on how they cracked it are too detailed.

Other Public Key

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.
   PRO Cracking EQUIV to factoring!

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.
   PRO Cracking EQUIV to factoring!
   CON Never used, Too slow.

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.
   PRO Cracking EQUIV to factoring!
   CON Never used, Too slow.
2. Goldwasser-Micali Enc: Cracking $\equiv$ SQRT mod pq.

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.
   PRO Cracking EQUIV to factoring!
   CON Never used, Too slow.
2. Goldwasser-Micali Enc: Cracking $\equiv$ SQRT mod pq.
   PRO Cracking EQUIV to a natural problem.

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.
   PRO Cracking EQUIV to factoring!
   CON Never used, Too slow.
2. Goldwasser-Micali Enc: Cracking $\equiv$ SQRT mod pq.
   PRO Cracking EQUIV to a natural problem.
   CON Never used, Too Slow.

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.
   PRO Cracking EQUIV to factoring!
   CON Never used, Too slow.
2. Goldwasser-Micali Enc: Cracking $\equiv$ SQRT mod pq.
   PRO Cracking EQUIV to a natural problem.
   CON Never used, Too Slow.
   NICK's CON Only transmits one friggin bit!

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.
   PRO Cracking EQUIV to factoring!
   CON Never used, Too slow.
2. Goldwasser-Micali Enc: Cracking $\equiv$ SQRT mod pq.
   PRO Cracking EQUIV to a natural problem.
   CON Never used, Too Slow.
   NICK's CON Only transmits one friggin bit!
3. Blum-Goldwater Enc: Cracking $\equiv$ Comp Secure PRG.

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.
   PRO Cracking EQUIV to factoring!
   CON Never used, Too slow.
2. Goldwasser-Micali Enc: Cracking $\equiv$ SQRT mod pq.
   PRO Cracking EQUIV to a natural problem.
   CON Never used, Too Slow.
   NICK's CON Only transmits one friggin bit!
3. Blum-Goldwater Enc: Cracking $\equiv$ Comp Secure PRG.
   PRO PRG's tie into other parts of the course

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.
   PRO Cracking EQUIV to factoring!
   CON Never used, Too slow.
2. Goldwasser-Micali Enc: Cracking $\equiv$ SQRT mod pq.
   PRO Cracking EQUIV to a natural problem.
   CON Never used, Too Slow.
   NICK's CON Only transmits one friggin bit!
3. Blum-Goldwater Enc: Cracking $\equiv$ Comp Secure PRG.
   PRO PRG's tie into other parts of the course
   PRO Uses Blum-Blum-Shub PRG. FUN to say **Blum-Blum-Shub**.

Other Public Key

1. Rabin Enc, and variants: Cracking $\equiv$ factoring.
   PRO Cracking EQUIV to factoring!
   CON Never used, Too slow.
2. Goldwasser-Micali Enc: Cracking $\equiv$ SQRT mod pq.
   PRO Cracking EQUIV to a natural problem.
   CON Never used, Too Slow.
   NICK's CON Only transmits one friggin bit!
3. Blum-Goldwater Enc: Cracking $\equiv$ Comp Secure PRG.
   PRO PRG's tie into other parts of the course
   PRO Uses Blum-Blum-Shub PRG. FUN to say **Blum-Blum-Shub**.
   NICK's CON Only transmits one friggin bit!

More Factoring Algorithms

More Factoring Algorithms

1. Quadratic Sieve Factoring.

More Factoring Algorithms

1. Quadratic Sieve Factoring.
   PRO Faster than Pollard's algorithm. Really used.

More Factoring Algorithms

1. Quadratic Sieve Factoring.
   PRO Faster than Pollard's algorithm. Really used.
   PRO I have awesome slide packets on it for 3 lectures.

More Factoring Algorithms

1. Quadratic Sieve Factoring.
   PRO Faster than Pollard's algorithm. Really used.
   PRO I have awesome slide packets on it for 3 lectures.
   CON This is **crypto** not friggin **Comp Number Theory**!

More Factoring Algorithms

1. Quadratic Sieve Factoring.
   PRO Faster than Pollard's algorithm. Really used.
   PRO I have awesome slide packets on it for 3 lectures.
   CON This is **crypto** not friggin **Comp Number Theory**!
2. Number Field Sieve Factoring.

More Factoring Algorithms

1. Quadratic Sieve Factoring.
   PRO Faster than Pollard's algorithm. Really used.
   PRO I have awesome slide packets on it for 3 lectures.
   CON This is **crypto** not friggin **Comp Number Theory**!
2. Number Field Sieve Factoring.
   PRO Faster than Quadratic Sieve. Best known algorithm.

More Factoring Algorithms

1. Quadratic Sieve Factoring.
   PRO Faster than Pollard's algorithm. Really used.
   PRO I have awesome slide packets on it for 3 lectures.
   CON This is **crypto** not friggin **Comp Number Theory**!
2. Number Field Sieve Factoring.
   PRO Faster than Quadratic Sieve. Best known algorithm.
   BILL'S CON Writeups are terrible. Don't know it yet.

Algorithm For Discrete Log

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
2. Pollard-Rho DL algorithm.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
2. Pollard-Rho DL algorithm.
   PRO Conceptually easy.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
2. Pollard-Rho DL algorithm.
   PRO Conceptually easy.
   CON Has some messy details.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
2. Pollard-Rho DL algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
3. Other Algorithms.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
2. Pollard-Rho DL algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
3. Other Algorithms.
   PRO Interesting.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
2. Pollard-Rho DL algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
3. Other Algorithms.
   PRO Interesting.
   CON Messy.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
2. Pollard-Rho DL algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
3. Other Algorithms.
   PRO Interesting.
   CON Messy.
   CON This is not a course on **Comp Number Theory**.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
2. Pollard-Rho DL algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
3. Other Algorithms.
   PRO Interesting.
   CON Messy.
   CON This is not a course on **Comp Number Theory**.
   CON In the future this might **become** a course in **Comp Number Theory**.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
2. Pollard-Rho DL algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
3. Other Algorithms.
   PRO Interesting.
   CON Messy.
   CON This is not a course on **Comp Number Theory**.
   CON In the future this might **become** a course in **Comp Number Theory**. Or on **Quantum Computing**.

Algorithm For Discrete Log

1. Baby-Step Giant-Step Algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
2. Pollard-Rho DL algorithm.
   PRO Conceptually easy.
   CON Has some messy details.
3. Other Algorithms.
   PRO Interesting.
   CON Messy.
   CON This is not a course on **Comp Number Theory**.
   CON In the future this might **become** a course in **Comp Number Theory**. Or on **Quantum Computing**. Or on **Machine Learning**.

More Secret Sharing with Cards

More Secret Sharing with Cards

There is a better way to do secret sharing with cards that transmits slightly more bits.

More Secret Sharing with Cards

There is a better way to do secret sharing with cards that transmits slightly more bits.

PRO I know it and I like it and its not that hard.

More Secret Sharing with Cards

There is a better way to do secret sharing with cards that transmits slightly more bits.

PRO I know it and I like it and its not that hard.

CON Esoteric!

More Secret Sharing with Cards

There is a better way to do secret sharing with cards that transmits slightly more bits.

PRO I know it and I like it and its not that hard.

CON Esoteric!

CAVEAT Raises the question of whats more important:

More Secret Sharing with Cards

There is a better way to do secret sharing with cards that transmits slightly more bits.

PRO I know it and I like it and its not that hard.

CON Esoteric!

CAVEAT Raises the question of whats more important:

1. **Messy protocols and attacks** that are used in the real world.

More Secret Sharing with Cards

There is a better way to do secret sharing with cards that transmits slightly more bits.

PRO I know it and I like it and its not that hard.

CON Esoteric!

CAVEAT Raises the question of whats more important:

1. **Messy protocols and attacks** that are used in the real world.
2. **Clean toy problems** that are interesting.

More Secret Sharing with Cards

There is a better way to do secret sharing with cards that transmits slightly more bits.

PRO I know it and I like it and its not that hard.

CON Esoteric!

CAVEAT Raises the question of whats more important:

1. **Messy protocols and attacks** that are used in the real world.
2. **Clean toy problems** that are interesting.

I prefer **Clean Toy Problems**.

More Secret Sharing with Cards

There is a better way to do secret sharing with cards that transmits slightly more bits.

PRO I know it and I like it and its not that hard.

CON Esoteric!

CAVEAT Raises the question of whats more important:

1. **Messy protocols and attacks** that are used in the real world.
2. **Clean toy problems** that are interesting.

I prefer **Clean Toy Problems**.

I may be wrong about this.

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.
   PRO Uses PRG's so ties into earlier part of the course.

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.
   PRO Uses PRG's so ties into earlier part of the course.
   PRO I already have slides for it!

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.
   PRO Uses PRG's so ties into earlier part of the course.
   PRO I already have slides for it!
   CON Shares of size $|s|$ seems quite fine.

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.
   PRO Uses PRG's so ties into earlier part of the course.
   PRO I already have slides for it!
   CON Shares of size $|s|$ seems quite fine.
   CON Messy!

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.
   PRO Uses PRG's so ties into earlier part of the course.
   PRO I already have slides for it!
   CON Shares of size $|s|$ seems quite fine.
   CON Messy!
2. **Recall** Info-Theoretic: we need all players honest.

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.
   PRO Uses PRG's so ties into earlier part of the course.
   PRO I already have slides for it!
   CON Shares of size $|s|$ seems quite fine.
   CON Messy!
2. **Recall** Info-Theoretic: we need all players honest.
   IF players have comp limits then can do Secret Sharing where we verify all telling the truth.

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.
   PRO Uses PRG's so ties into earlier part of the course.
   PRO I already have slides for it!
   CON Shares of size $|s|$ seems quite fine.
   CON Messy!
2. **Recall** Info-Theoretic: we need all players honest.
   IF players have comp limits then can do Secret Sharing where we verify all telling the truth.
   PRO I already have slides for it!

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.
   PRO Uses PRG's so ties into earlier part of the course.
   PRO I already have slides for it!
   CON Shares of size $|s|$ seems quite fine.
   CON Messy!
2. **Recall** Info-Theoretic: we need all players honest.
   IF players have comp limits then can do Secret Sharing where we verify all telling the truth.
   PRO I already have slides for it!
   CON If Putin can't trust people then I don't think he wants to learn the math to avoid this problem.

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.
   PRO Uses PRG's so ties into earlier part of the course.
   PRO I already have slides for it!
   CON Shares of size $|s|$ seems quite fine.
   CON Messy!
2. **Recall** Info-Theoretic: we need all players honest.
   IF players have comp limits then can do Secret Sharing where we verify all telling the truth.
   PRO I already have slides for it!
   CON If Putin can't trust people then I don't think he wants to learn the math to avoid this problem.
   CON Messy!

Computational Secret Sharing

We did **Information-Theoretic Secret Sharing**

1. **Recall** Info-Theoretic: shares are size $\geq |s|$.
   IF give the players comp limits then can do Secret Sharing with shares of size $\leq \beta|s|$ where $\beta < 1$.
   PRO Uses PRG's so ties into earlier part of the course.
   PRO I already have slides for it!
   CON Shares of size $|s|$ seems quite fine.
   CON Messy!
2. **Recall** Info-Theoretic: we need all players honest.
   IF players have comp limits then can do Secret Sharing where we verify all telling the truth.
   PRO I already have slides for it!
   CON If Putin can't trust people then I don't think he wants to learn the math to avoid this problem.
   CON Messy!
   CON Both Esoteric, thought not as much as the cards-stuff.

Non-Ideal Secret Sharing

Prove that certain access structures **cannot** have Ideal secret Sharing.

Non-Ideal Secret Sharing

Prove that certain access structures **cannot** have Ideal secret Sharing.

More Fun for Me then for You!

Other Real World Material

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!
   CON Really Really Boring!

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!
   CON Really Really Boring!
3. Bitcoin.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!
   CON Really Really Boring!
3. Bitcoin.
   PRO Hot topic.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!
   CON Really Really Boring!
3. Bitcoin.
   PRO Hot topic.
   PRO Uses other parts of the course.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!
   CON Really Really Boring!
3. Bitcoin.
   PRO Hot topic.
   PRO Uses other parts of the course.
   CON Bitcoin is a Ponzi Scheme.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!
   CON Really Really Boring!
3. Bitcoin.
   PRO Hot topic.
   PRO Uses other parts of the course.
   CON Bitcoin is a Ponzi Scheme.
4. Security of Electronic Voting.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!
   CON Really Really Boring!
3. Bitcoin.
   PRO Hot topic.
   PRO Uses other parts of the course.
   CON Bitcoin is a Ponzi Scheme.
4. Security of Electronic Voting.
   PRO Hot topic.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!
   CON Really Really Boring!
3. Bitcoin.
   PRO Hot topic.
   PRO Uses other parts of the course.
   CON Bitcoin is a Ponzi Scheme.
4. Security of Electronic Voting.
   PRO Hot topic.
   PRO Uses other parts of the course.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!
   CON Really Really Boring!
3. Bitcoin.
   PRO Hot topic.
   PRO Uses other parts of the course.
   CON Bitcoin is a Ponzi Scheme.
4. Security of Electronic Voting.
   PRO Hot topic.
   PRO Uses other parts of the course.
   CON Very detailed protocols.

Other Real World Material

1. Digital Signatures: Proving that Irene send the email calling Bill a crazy croissant.
   PRO Really Used.
   CON Really Boring.
2. MD5 and other stream ciphers that are really used.
   PRO Really Really Used!
   CON Really Really Boring!
3. Bitcoin.
   PRO Hot topic.
   PRO Uses other parts of the course.
   CON Bitcoin is a Ponzi Scheme.
4. Security of Electronic Voting.
   PRO Hot topic.
   PRO Uses other parts of the course.
   CON Very detailed protocols.
   CON Other problems with voting— gerrymandering, disenfranchisement, replacing non-partisan voter commissioners with lackeys.

Proofs of Security, More Rigor

No Fun for me or for you.