

17/08/2021

CS 6160 Cryptology Lecture 0: Introduction & Logistics

Maria Francis

August 17, 2021

17/08/2021

Welcome to Cryptology

- Introductory course on Cryptography and Cryptanalysis.

17/08/2021

Welcome to Cryptology

- Introductory course on Cryptography and Cryptanalysis.
- It is a theoretical course.

17/08/2021

Welcome to Cryptology

- Introductory course on Cryptography and Cryptanalysis.
- It is a theoretical course.
- We will cover the basics of modern cryptography like one-way functions, provable security, reductionist arguments.

Welcome to Cryptology

- Introductory course on Cryptography and Cryptanalysis.
- It is a theoretical course.
- We will cover the basics of modern cryptography like one-way functions, provable security, reductionist arguments.
- We then give an overview of symmetric key cryptography, public key cryptography (PKC) and then look at some advanced techniques like zero-knowledge proofs, anonymous credentials and post quantum crypto.

17/08/2021

Prerequisites

- No prerequisites other than discrete mathematics is officially required.

Prerequisites

- No prerequisites other than discrete mathematics is officially required.
- But it is good to know basics of probability (e.g: random variable, discrete probability distributions) and computational complexity (e.g: NP, NP completeness, polynomial time reductions)

Prerequisites

- No prerequisites other than discrete mathematics is officially required.
- But it is good to know basics of probability (e.g: random variable, discrete probability distributions) and computational complexity (e.g: NP, NP completeness, polynomial time reductions)
- The number theory required will be covered in class but this is a good basic resource: <http://www.hyperelliptic.org/tanja/teaching/cryptoI13/nt.pdf>

Syllabus

Classic cryptosystems, perfect secrecy, one-way functions, pseudo random generators, private and public key cryptography, collision resistant hashing, PKI, digital signatures, secret sharing schemes and zero knowledge proofs.

Introduction to Cryptanalysis, Attacks on block ciphers : exhaustive search, time-space tradeoffs, differential & linear cryptanalysis, meet in the middle, Attacks on public key systems: Integer factoring, Cryptanalysis of Hash functions, Overview of side channel attacks

References

- Cryptography - Theory and Practice by D. Stinson. A standard textbook.
- Introduction to Modern Cryptography - J. Katz and Y. Lindell. A new textbook with a very modern take.
- A Graduate Course in Applied Cryptography - D. Boneh, V. Shoup. More practical engineering!
- The Foundations of Cryptography - Vol 1 – O. Goldreich. For the theoretical foundations of modern crypto, a good reference for one-way functions and ZK proofs.
- An introduction to number theory and cryptography – N. Koblitz. For the number theory used in crypto.
- "The Code Book" by S. Singh & "The Codebreakers" by D. Kahn. Both chronicle the history of crypto.

Other References

- Lecture notes by
 - ▶ Shafi Goldwasser and Mihir Bellare (collected into a single document but slightly old),
 - ▶ Rafael Pass and Abhi Shelat (collected into a single document), and many many more.

Other References

- Lecture notes by
 - ▶ Shafi Goldwasser and Mihir Bellare (collected into a single document but slightly old),
 - ▶ Rafael Pass and Abhi Shelat (collected into a single document), and many many more.
- Explore and utilize all resources -
 - ▶ lecture notes,
 - ▶ video lectures (from reputed sources like university lectures, Simons Institute, Institute for Advanced Study, etc),
 - ▶ papers published at top venues like **Crypto**, **Eurocrypt**, **Asiacrypt**, **Indocrypt**, etc and journals like **Designs**, **Codes and Cryptography**, **Journal of Cryptology** etc.

17/08/2021

Online Classes

- We meet using this Google meet link : E slot, Tues (10 : 00 – 10 : 55), Thurs (12 : 00 – 12 : 55) and Fri (9 : 00 – 9 : 55).
- The videos of the lectures will be uploaded on YouTube (mostly during the Thurs slot), links will be provided in Google classroom.
- Please view the video lecture BEFORE you come to class

Online Classes

- We meet using this Google meet link : E slot, Tues (10 : 00 – 10 : 55), Thurs (12 : 00 – 12 : 55) and Fri (9 : 00 – 9 : 55).
- The videos of the lectures will be uploaded on YouTube (mostly during the Thurs slot), links will be provided in Google classroom.
- Please view the video lecture BEFORE you come to class
- A problem set will also be posted.

Online Classes

- We meet using this Google meet link : E slot, Tues (10 : 00 – 10 : 55), Thurs (12 : 00 – 12 : 55) and Fri (9 : 00 – 9 : 55).
- The videos of the lectures will be uploaded on YouTube (mostly during the Thurs slot), links will be provided in Google classroom.
- Please view the video lecture BEFORE you come to class
- A problem set will also be posted.
- Every Tuesday we meet to discuss the video lecture and the problem set.

Online Classes

- We meet using this Google meet link : E slot, Tues (10 : 00 – 10 : 55), Thurs (12 : 00 – 12 : 55) and Fri (9 : 00 – 9 : 55).
- The videos of the lectures will be uploaded on YouTube (mostly during the Thurs slot), links will be provided in Google classroom.
- **Please view the video lecture BEFORE you come to class**
- A problem set will also be posted.
- Every Tuesday we meet to discuss the video lecture and the problem set.
- We will have a quiz on the topics the following Friday.

Online Classes

- We meet using this Google meet link : E slot, Tues (10 : 00 – 10 : 55), Thurs (12 : 00 – 12 : 55) and Fri (9 : 00 – 9 : 55).
- The videos of the lectures will be uploaded on YouTube (mostly during the Thurs slot), links will be provided in Google classroom.
- **Please view the video lecture BEFORE you come to class**
- A problem set will also be posted.
- Every Tuesday we meet to discuss the video lecture and the problem set.
- We will have a quiz on the topics the following Friday.
- Attendance will be taken, 10% of your final grade!
- TAs for this course: will be announced soon.

Evaluation!!

- Attendance - **10%** ($\leq \frac{1}{3}$ - 0 marks, $\leq \frac{2}{3}$ - 6 marks, $\geq \frac{2}{3}$ - 10 marks).
- Quizzes - **50%** (Previously announced, mostly every week, online 10 minute quizzes)
- Paper presentation by a video, Report of a paper - **20% + 20% = 40%**

Evaluation!!

- Attendance - **10%** ($\leq \frac{1}{3}$ - 0 marks, $\leq \frac{2}{3}$ - 6 marks, $\geq \frac{2}{3}$ - 10 marks).
- Quizzes - **50%** (Previously announced, mostly every week, online 10 minute quizzes)
- Paper presentation by a video, Report of a paper - **$20\% + 20\% = 40\%$**
- Not a perfect method!

Evaluation!!

- Attendance - **10%** ($\leq \frac{1}{3}$ - 0 marks, $\leq \frac{2}{3}$ - 6 marks, $\geq \frac{2}{3}$ - 10 marks).
- Quizzes - **50%** (Previously announced, mostly every week, online 10 minute quizzes)
- Paper presentation by a video, Report of a paper - **20% + 20% = 40%**
- Not a perfect method!
- **Plagiarism or any form of cheating will be an automatic F and will be reported to the dept.**

Quizzes

- Will be given as a Quiz Assignment (MCQs and short answers) in Google classroom/SAFE app.
- After it is assigned you will have **ten minutes** to give your answers.
- Dates of the quizzes will be announced in advance.
- The plan is to conduct approx. 12 (could be more or less) quizzes and **to account for network issues we will not consider 3 of them.**

17/08/2021

Paper Presentation

- Link for the list of papers will be shared.

17/08/2021

Paper Presentation

- Link for the list of papers will be shared.
- You need to make a 10 min video recording of the presentation of the paper and share it with the class.

17/08/2021

Paper Presentation

- Link for the list of papers will be shared.
- You need to make a 10 min video recording of the presentation of the paper and share it with the class.
- The presentation should include - motivation, main result, what is innovative or different about the approach, significance, what work has followed this work, etc.

Paper Presentation

- Link for the list of papers will be shared.
- You need to make a 10 min video recording of the presentation of the paper and share it with the class.
- The presentation should include - motivation, main result, what is innovative or different about the approach, significance, what work has followed this work, etc.
- The more insightful the presentation and report the better your marks.

Paper Presentation

- Link for the list of papers will be shared.
- You need to make a 10 min video recording of the presentation of the paper and share it with the class.
- The presentation should include - motivation, main result, what is innovative or different about the approach, significance, what work has followed this work, etc.
- The more insightful the presentation and report the better your marks.
- To score more :
 - ▶ Include more pictorial representations of the material to reflect your understanding,
 - ▶ Show the progress in this area so far and also the progress in the area post this paper, etc.

17/08/2021

Paper Presentation

- **Preferably** use Beamer (a LaTeX document class for presentation slides) not Powerpoint to make your presentation especially when you have a lot of math!

Paper Presentation

- **Preferably** use Beamer (a LaTeX document class for presentation slides) not Powerpoint to make your presentation especially when you have a lot of math!
- Put very little text on one slide - $\approx 7 - 8$ lines in a slides and preferably phrases, not sentences!

Paper Presentation

- **Preferably** use Beamer (a LaTeX document class for presentation slides) not Powerpoint to make your presentation especially when you have a lot of math!
- Put very little text on one slide - $\approx 7 - 8$ lines in a slides and preferably phrases, not sentences!
- 10 min presentation would mean not more than 10 – 15 slides!

Paper Presentation

- **Preferably** use Beamer (a LaTeX document class for presentation slides) not Powerpoint to make your presentation especially when you have a lot of math!
- Put very little text on one slide - $\approx 7 - 8$ lines in a slides and preferably phrases, not sentences!
- 10 min presentation would mean not more than 10 – 15 slides!
- Do not go into the details of proofs. Even if you want to, **give only the main ideas!**

Paper Presentation

- **Preferably** use Beamer (a LaTeX document class for presentation slides) not Powerpoint to make your presentation especially when you have a lot of math!
- Put very little text on one slide - $\approx 7 - 8$ lines in a slides and preferably phrases, not sentences!
- 10 min presentation would mean not more than 10 – 15 slides!
- Do not go into the details of proofs. Even if you want to, **give only the main ideas!**
- In the report you can go into details **but again no copying as-is from the original paper!**

Paper Presentation

- **Preferably** use Beamer (a LaTeX document class for presentation slides) not Powerpoint to make your presentation especially when you have a lot of math!
- Put very little text on one slide - $\approx 7 - 8$ lines in a slides and preferably phrases, not sentences!
- 10 min presentation would mean not more than 10 – 15 slides!
- Do not go into the details of proofs. Even if you want to, **give only the main ideas!**
- In the report you can go into details **but again no copying as-is from the original paper!**
- It is okay not to understand all the details given in the paper but the more you understand the better your report and your presentation.

17/08/2021

Report

- Two page report typeset by LaTeX tools.

17/08/2021

Report

- Two page report **typeset by LaTeX tools**.
 - ▶ If it is not compiled using LaTeX the assignment will be awarded a 0.

17/08/2021

Report

- Two page report **typeset by LaTeX tools**.
 - ▶ If it is not compiled using LaTeX the assignment will be awarded a 0.
- Lots of online resources for LaTeX tools such as:
<http://web.mit.edu/rsi/www/pdfs/new-latex.pdf>

Report

- Two page report **typeset by LaTeX tools**.
 - ▶ If it is not compiled using LaTeX the assignment will be awarded a 0.
- Lots of online resources for LaTeX tools such as:
<http://web.mit.edu/rsi/www/pdfs/new-latex.pdf>
- Material cannot be copy pasted from the original paper - it should reflect your understanding!

Report

- Two page report **typeset by LaTeX tools**.
 - ▶ If it is not compiled using LaTeX the assignment will be awarded a 0.
- Lots of online resources for LaTeX tools such as:
<http://web.mit.edu/rsi/www/pdfs/new-latex.pdf>
- Material cannot be copy pasted from the original paper - it should reflect your understanding!
- This is a possible template:

Report

- Two page report **typeset by LaTeX tools**.
 - ▶ If it is not compiled using LaTeX the assignment will be awarded a 0.
- Lots of online resources for LaTeX tools such as:
<http://web.mit.edu/rsi/www/pdfs/new-latex.pdf>
- Material cannot be copy pasted from the original paper - it should reflect your understanding!
- This is a possible template:
 - ▶ **Pick a main idea/proof and explain just that in your own language**

Report

- Two page report **typeset by LaTeX tools**.
 - ▶ If it is not compiled using LaTeX the assignment will be awarded a 0.
- Lots of online resources for LaTeX tools such as:
<http://web.mit.edu/rsi/www/pdfs/new-latex.pdf>
- Material cannot be copy pasted from the original paper - it should reflect your understanding!
- This is a possible template:
 - ▶ **Pick a main idea/proof and explain just that in your own language**
 - ▶ **Explain the challenges –**

Report

- Two page report **typeset by LaTeX tools**.
 - ▶ If it is not compiled using LaTeX the assignment will be awarded a 0.
- Lots of online resources for LaTeX tools such as:
<http://web.mit.edu/rsi/www/pdfs/new-latex.pdf>
- Material cannot be copy pasted from the original paper - it should reflect your understanding!
- This is a possible template:
 - ▶ **Pick a main idea/proof and explain just that in your own language**
 - ▶ **Explain the challenges – E.g: what if we are trying to prove the same result/problem without this new idea/technique.**

Report

- Two page report **typeset by LaTeX tools**.
 - ▶ If it is not compiled using LaTeX the assignment will be awarded a 0.
- Lots of online resources for LaTeX tools such as:
<http://web.mit.edu/rsi/www/pdfs/new-latex.pdf>
- Material cannot be copy pasted from the original paper - it should reflect your understanding!
- This is a possible template:
 - ▶ **Pick a main idea/proof and explain just that in your own language**
 - ▶ **Explain the challenges – E.g: what if we are trying to prove the same result/problem without this new idea/technique.**
 - ▶ **Related work done before and after this work? –**

Report

- Two page report **typeset by LaTeX tools**.
 - ▶ If it is not compiled using LaTeX the assignment will be awarded a 0.
- Lots of online resources for LaTeX tools such as:
<http://web.mit.edu/rsi/www/pdfs/new-latex.pdf>
- Material cannot be copy pasted from the original paper - it should reflect your understanding!
- This is a possible template:
 - ▶ **Pick a main idea/proof and explain just that in your own language**
 - ▶ **Explain the challenges – E.g: what if we are trying to prove the same result/problem without this new idea/technique.**
 - ▶ **Related work done before and after this work? – One way to find out: Google Scholar!**

17/08/2021

Instructions Contd!

17/08/2021

Instructions Contd!

- The deadline to email **the instructor and the TAs**, the paper you want to present and write a report will be informed.

17/08/2021

Instructions Contd!

- The deadline to email **the instructor and the TAs**, the paper you want to present and write a report will be informed.
- These papers are difficult papers and **you will need ATLEAST a month to read and fully understand them.**

Instructions Contd!

- The deadline to email **the instructor and the TAs**, the paper you want to present and write a report will be informed.
- These papers are difficult papers and **you will need ATLEAST a month to read and fully understand them. So start early!**

17/08/2021

Conclusion

- You can identify a **totally different paper** to present but you will need my approval!

Conclusion

- You can identify a **totally different paper** to present but you will need my approval!
- Reading (and understanding) a paper is tough - you will have ample time, so utilize it effectively!

Conclusion

- You can identify a **totally different paper** to present but you will need my approval!
- Reading (and understanding) a paper is tough - you will have ample time, so utilize it effectively!
- Do not think you only have to read that paper and summarize. **Marking will be stringent and based on how much you have understood the area not just that paper and the techniques the paper introduces.**

Conclusion

- You can identify a **totally different paper** to present but you will need my approval!
- Reading (and understanding) a paper is tough - you will have ample time, so utilize it effectively!
- Do not think you only have to read that paper and summarize. **Marking will be stringent and based on how much you have understood the area not just that paper and the techniques the paper introduces.**
- **Explore all the resources related to the paper to understand the work better.** For e.g: presentations given by the author about this work or a related work.

Conclusion

- You can identify a **totally different paper** to present but you will need my approval!
- Reading (and understanding) a paper is tough - you will have ample time, so utilize it effectively!
- Do not think you only have to read that paper and summarize. **Marking will be stringent and based on how much you have understood the area not just that paper and the techniques the paper introduces.**
- **Explore all the resources related to the paper to understand the work better.** For e.g: presentations given by the author about this work or a related work.
- One resource on reading a paper :
<https://users.ece.cmu.edu/~vsekar/Teaching/Spring20/18731/reading/howtoread.pdf>