

CSE 539  
Applied Cryptography  
Fall 2024

Ni Trieu (ASU)

# Week-1

- Greetings
- Syllabus
- What Cryptography is
- What “Applied” Cryptography is
- Why cryptography is good for the world?

# Greetings

---

## CSE 539: Applied Cryptography

Fall 2024 (Internet - Hybrid; M 9:00 - 10:15 SCOB228)

---

- Instructor: Ni Trieu ([nitrieu@asu.edu](mailto:nitrieu@asu.edu))
- TA: Jiahui Gao ([jgao76@asu.edu](mailto:jgao76@asu.edu))

Office hours: 15:00-16:00 Wednesday at Bio-design Building B or via <https://asu.zoom.us/my/TBA>

- Grader: Raj Subash Mendon ([rmendon1@asu.edu](mailto:rmendon1@asu.edu))
- Grader: Hartik Suhagiya ([hmsuhagi@asu.edu](mailto:hmsuhagi@asu.edu))

# Greetings

- “Hybrid course” => means
  - Its delivery is via a combination of in-person meetings and online assignments.
  - All course materials including lectures and assignments, will be predominantly delivered in an online setting. I will be posting new materials every **Wednesday**.
- Textbook
  - The Joy of Cryptography; Mike Rosulek; <https://joyofcryptography.com/>
  - Introduction to Modern Cryptography (2nd edition); Jonathan Katz and Yehuda Lindell; <http://www.cs.umd.edu/~jkatz/imc.html>
  - Handbook of Applied Cryptograph; Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone; <https://cacr.uwaterloo.ca/hac/>
  - A Pragmatic Introduction to Secure Multi-Party Computation; David Evans, Vladimir Kolesnikov, Mike Rosulek; <https://securecomputation.org/>

# Syllabus: Course content

Won't cover	Will cover
	<ul style="list-style-type: none"><li>- Basics of cryptography</li></ul>

# Syllabus: Course content

<b>Won't cover</b>	<b>Will cover</b>
<ul style="list-style-type: none"><li>- Software security</li></ul>	<ul style="list-style-type: none"><li>- Basics of cryptography</li></ul>

# Syllabus: Course content

Won't cover	Will cover
<ul style="list-style-type: none"><li>- Software security</li></ul>	<ul style="list-style-type: none"><li>- Basics of cryptography</li><li>- Implementation of crypto primitives</li></ul>

# Syllabus: Course content

Won't cover	Will cover
<ul style="list-style-type: none"><li>- Software security</li><li>- Implementation of how to hack an app</li></ul>	<ul style="list-style-type: none"><li>- Basics of cryptography</li><li>- Implementation of crypto primitives</li></ul>



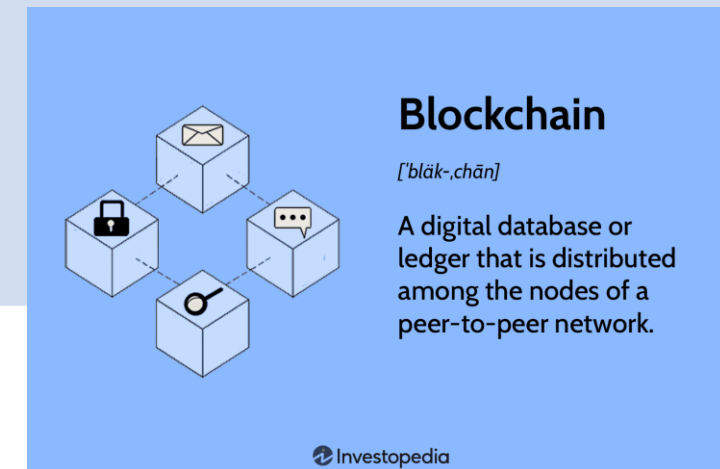
# Syllabus: Course content

## Won't cover

- Software security
- Implementation of how to hack an app

## Will cover

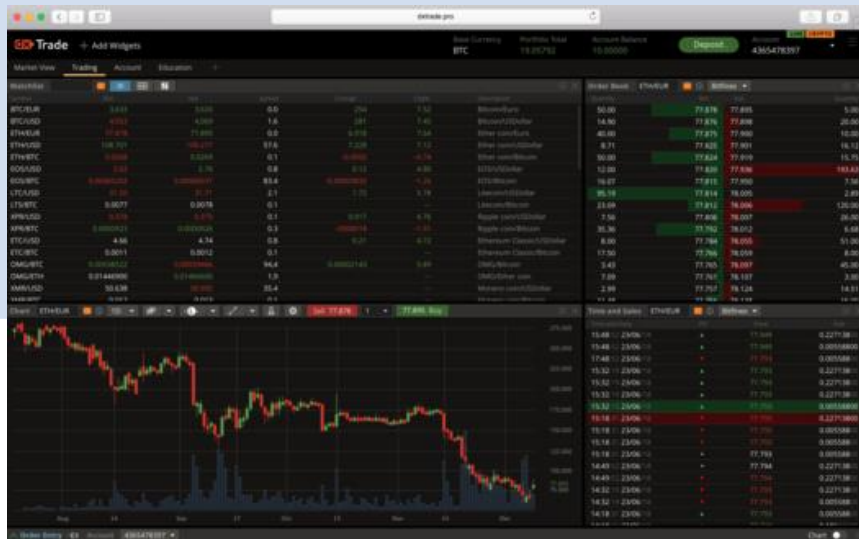
- Basics of cryptography
- Implementation of crypto primitives
- Applied crypto such as how cryptocurrency/blockchain works



# Syllabus: Course content

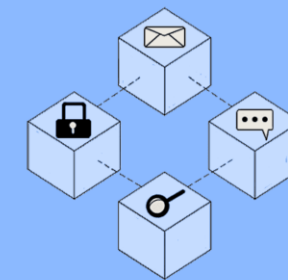
## Won't cover

- Software security
- Implementation of how to hack an app
- Other topics such as how to trade bitcoin 😊



## Will cover

- Basics of cryptography
- Implementation of crypto primitives
- Applied crypto such as how cryptocurrency/blockchain works



## Blockchain

[ˈblæk-,chān]

A digital database or ledger that is distributed among the nodes of a peer-to-peer network.

# Syllabus: Tentative Course Itinerary

## 1. Introduction (2 lectures):

- Overview of modern crypto and topics to be discussed in the class
- Overview of applied crypto and its implementations in real-world scenarios.

## 2. Basics of cryptography(10 lectures):

- Secret sharing scheme
- Provable Security/Security definition
- Pseudorandom Generators/Functions
- Block Ciphers
- Message Authentication Codes
- Hash Functions
- RSA/Digital Signatures
- Diffie-Hellman Key Agreement
- Public-Key Encryption

## 3. Advanced/applied cryptography (10 lectures):

- Multi-party secure computation (2)
- Homomorphic encryption (2)
- Zero-knowledge proof/blockchain (2)
- Privacy-preserving machine learning (2 lectures)
- Private database query (1 lecture)
- Other practical problems (1 lecture)

## 4. Final project presentations (8 lectures)

# Grading

1. **Homework (45%)**: Expect 3 online quizzes with a mixture of math, computation, security proofs, attacks, and problem-solving.
2. **Take-home Midterm Exam (25%)**: Focus on the basics of cryptography (theory or implementation)
3. **Final project and presentation (30%)**: A group of (3-4) students will choose to summarize a crypto paper and together write a 4-6 page report (without using Chat-GPT). The 10-minute presentation will be recorded by each group and will be available on Canvas.
4. **Bonus (1%)**: This rewards you for identifying bugs, mistakes, or similar issues in my lectures. For each bug you find, you will earn 25 points, up to a total of 100 points. This bonus assignment can contribute a maximum of 1% to your overall final grade. If you achieve the highest possible scores in your homework, exams, projects, and this bonus assignment, your final score will be 101 out of 100.



A+	A	A-	B+	B	C+	C	D	E
≥ 98%	≥ 95%	≥ 90%	≥ 88%	≥ 80%	≥ 75%	≥ 70%	≥ 60%	0 – 59%

# Final Project and Presentation

- A group of (3-4) students will choose to summarize a crypto paper and together write a 4-6 page report (without using ChatGPT). The 10-minute presentation will be recorded by each group and will be available on Canvas.
- Choose any project topic related to applied cryptography:
  - [https://docs.google.com/spreadsheets/d/1yQE\\_lhEN1YYO08plicYo8vWEAQR1xqoj83nzhvexQBU4/edit?usp=sharing](https://docs.google.com/spreadsheets/d/1yQE_lhEN1YYO08plicYo8vWEAQR1xqoj83nzhvexQBU4/edit?usp=sharing)
- The selected paper must be selected from top 20 conferences + journals
  - [https://scholar.google.es/citations?view\\_op=top\\_venues&hl=en&vq=eng\\_computersecuritycryptography](https://scholar.google.es/citations?view_op=top_venues&hl=en&vq=eng_computersecuritycryptography)
  - If you choose a topic related to your research direction (such as secure IoT), you can choose papers from top conferences/journals from your domain (e.g., INFOCOM, IEEE/ACM Transactions, <http://csrankings.org/>). Please send me an email for approval.

# Timeline

## Course Summary:

Date	Details	Due
Sat Sep 30, 2023	 HW1	due by 11:59pm
Sat Oct 21, 2023	 HW2	due by 11:59pm
Sat Nov 4, 2023	 Mid-term Exam	due by 11:59pm
Thu Nov 23, 2023	 HW3	due by 11:59pm
Fri Dec 1, 2023	 Project	due by 11:59pm

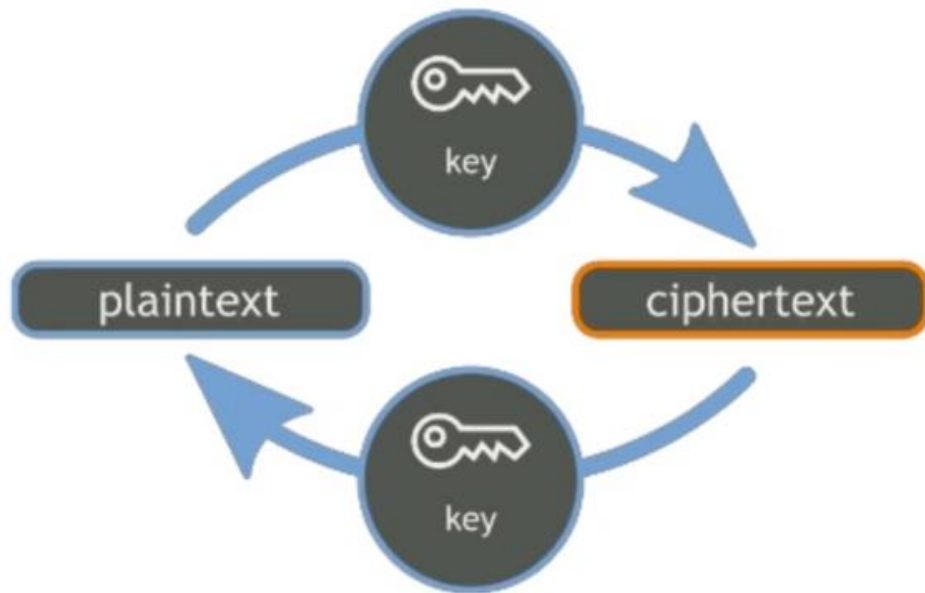
# Week-1

- ~~Greetings~~
- ~~Syllabus~~
- What Cryptography is
- What “Applied” Cryptography is
- Why cryptography is good for the world?

# What is Cryptography?

- Cryptography is more than just hiding information (i.e., encryption)
- Cryptography is math
- Crypto definition
  - Idea: compare 2 probability distributions

One-time Pad:

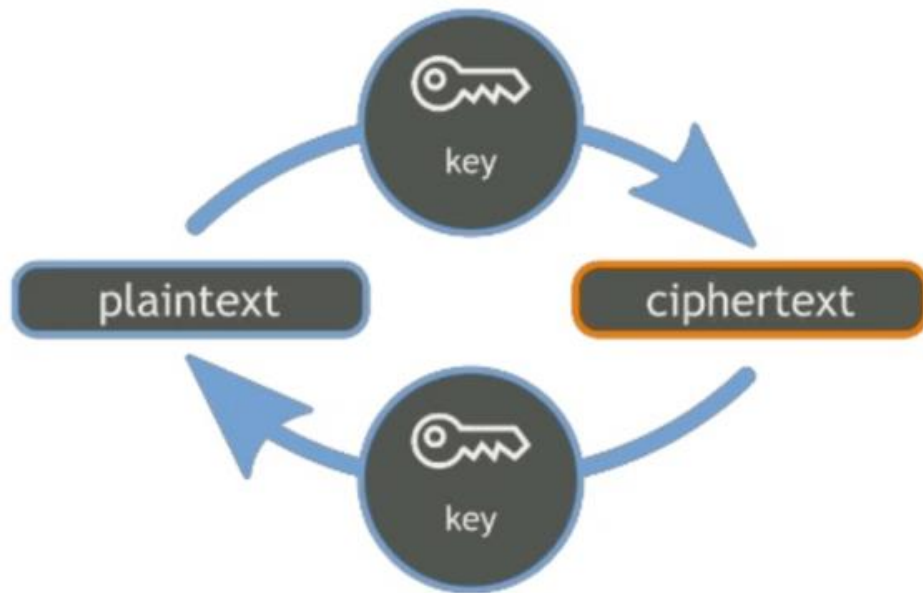




# What is Cryptography?

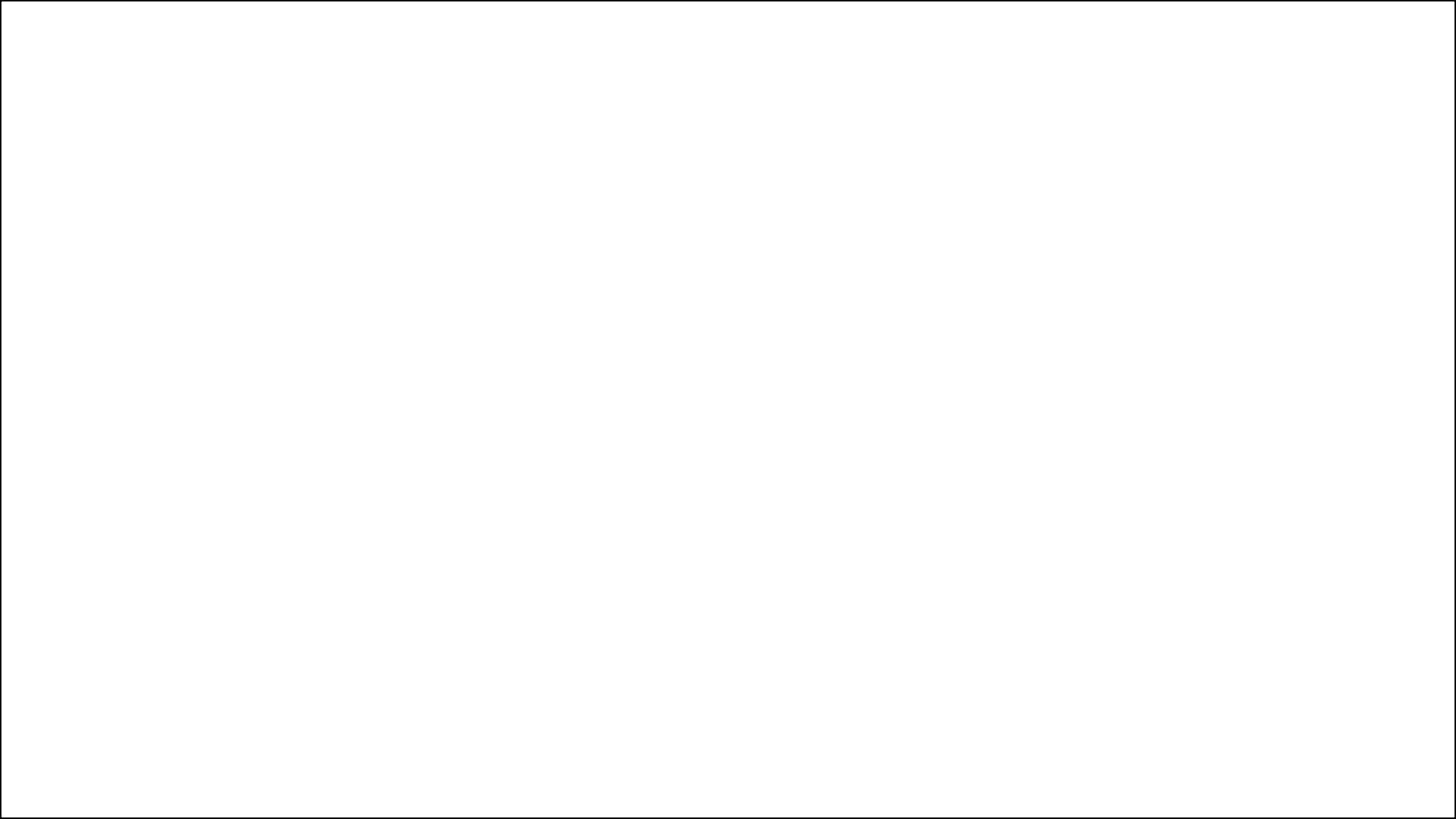
- Cryptography is more than just hiding information (i.e., encryption)
- Cryptography is math
- Crypto definition
  - Idea: compare 2 probability distributions

One-time Pad:







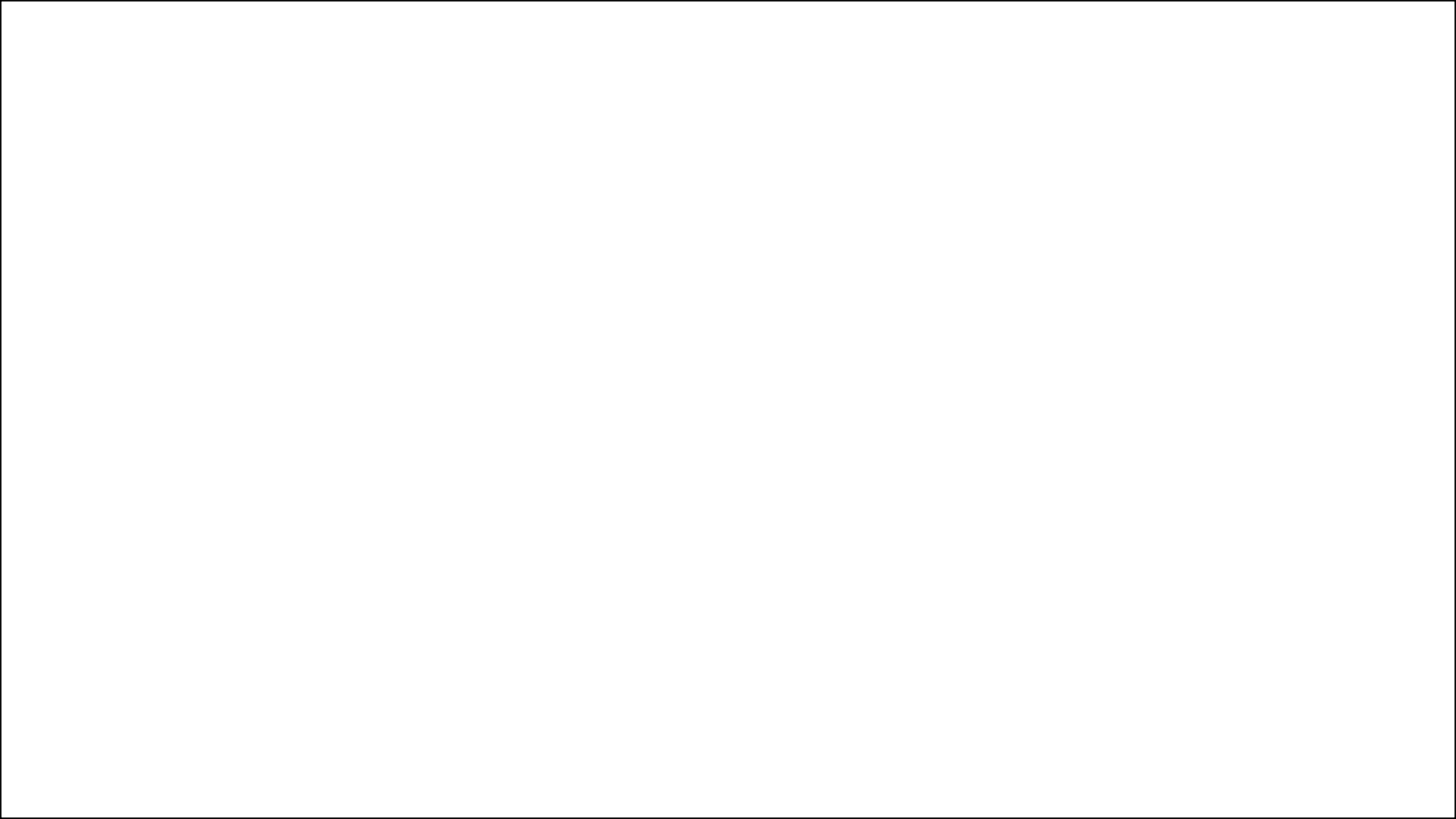


# Sample: Quiz Question

- Given an OTP ciphertext 1111, encrypted with the key 0101, what is the plaintext?
  - 0000
  - 1011
  - 0101
  - 1010

# Sample: Quiz Question

- Given two OTP ciphertexts, encrypted with the same key
  - $Ct = 01010100\ 01010001\ 01011010$
  - $ct' = 01010100\ 01001010\ 01000011$
- You know that either  $ct$  and  $ct'$  are encryptions of ``abc'' and ``ayz'' or  $ct$  and  $ctx'$  are encryptions of ``abz'' and ``xyz''
- Which of these two possibilities is correct?
  - ``abc'' and ``ayz''
  - ``abz'' and ``xyz''



# Week-1

- ~~Greetings~~
- ~~Syllabus~~
- ~~What Cryptography is~~
- What “Applied” Cryptography is
- Why cryptography is good for the world?