BILL RECORDED LECTURE

REVIEW FOR FINAL

FINAL REVIEW-ADMIN

Final Review-Admin

1) Final is Friday Dec 17 8:00PM-10:00PM. Take in the comfort of your home. I will be on zoom.

Final Review-Admin

1) Final is Friday Dec 17 8:00PM-10:00PM. Take in the comfort of your home. I will be on zoom.

2) Will be at course website at 7:55 or so. Will be dealt with **just like a HW**.

Final Review-Admin

1) Final is Friday Dec 17 8:00PM-10:00PM. Take in the comfort of your home. I will be on zoom.

2) Will be at course website at 7:55 or so. Will be dealt with **just like a HW**.

3) Open Notes, Open Book, Ope Web. You **cannot** call a friend.

Final Review-Admin

1) Final is Friday Dec 17 8:00PM-10:00PM. Take in the comfort of your home. I will be on zoom.

2) Will be at course website at 7:55 or so. Will be dealt with **just like a HW**.

3) Open Notes, Open Book, Ope Web. You **cannot** call a friend.

4) Coverage: Slides/HW. Comprehensive.

Final Review-Admin

1) Final is Friday Dec 17 8:00PM-10:00PM. Take in the comfort of your home. I will be on zoom.

2) Will be at course website at 7:55 or so. Will be dealt with **just like a HW**.

3) Open Notes, Open Book, Ope Web. You **cannot** call a friend.

4) Coverage: Slides/HW. Comprehensive.

5) Not on Exam: Guest Lectures, Alice-Bob-Love-Cards, Alice-Bob-Eve-Secret-Sharing-WITH CARDS. (note—normal secret sharing could be on the exam).

Final Review-Admin

1) Final is Friday Dec 17 8:00PM-10:00PM. Take in the comfort of your home. I will be on zoom.

2) Will be at course website at 7:55 or so. Will be dealt with **just like a HW**.

3) Open Notes, Open Book, Ope Web. You **cannot** call a friend.

4) Coverage: Slides/HW. Comprehensive.

5) Not on Exam: Guest Lectures, Alice-Bob-Love-Cards, Alice-Bob-Eve-Secret-Sharing-WITH CARDS. (note—normal secret sharing could be on the exam).

6) We hope to have grades on final and in course on Monday.

Final Review-Admin

1) Final is Friday Dec 17 8:00PM-10:00PM. Take in the comfort of your home. I will be on zoom.

2) Will be at course website at 7:55 or so. Will be dealt with **just like a HW**.

3) Open Notes, Open Book, Ope Web. You **cannot** call a friend.

4) Coverage: Slides/HW. Comprehensive.

5) Not on Exam: Guest Lectures, Alice-Bob-Love-Cards, Alice-Bob-Eve-Secret-Sharing-WITH CARDS. (note—normal secret sharing could be on the exam).

6) We hope to have grades on final and in course on Monday.

7) If time bad OR have special circumstances tell me ASAP.

Final Review-Admin

1) Final is Friday Dec 17 8:00PM-10:00PM. Take in the comfort of your home. I will be on zoom.

2) Will be at course website at 7:55 or so. Will be dealt with **just like a HW**.

3) Open Notes, Open Book, Ope Web. You **cannot** call a friend.

4) Coverage: Slides/HW. Comprehensive.

5) Not on Exam: Guest Lectures, Alice-Bob-Love-Cards, Alice-Bob-Eve-Secret-Sharing-WITH CARDS. (note—normal secret sharing could be on the exam).

6) We hope to have grades on final and in course on Monday.

7) If time bad OR have special circumstances tell me ASAP.

8) **Advice** Understand rather than memorize.

One-Letter Sub Ciphers

Shift, Affine, Gen Sub

1. **Shift** is x goes to $x + s \pmod{26}$.
2. **Affine** is x goes to $ax + b \pmod{26}$. a is rel prime to 26.
3. **Gen Sub** uses a random perm f and then x goes to $f(x)$.
4. **Keyword-Shift** uses a letter and a word and is supposed to look random.

Shift, Affine, Gen Sub

1. **Shift** is x goes to $x + s \pmod{26}$.
2. **Affine** is x goes to $ax + b \pmod{26}$. a is rel prime to 26.
3. **Gen Sub** uses a random perm f and then x goes to $f(x)$.
4. **Keyword-Shift** uses a letter and a word and is supposed to look random.

1. All need IS-ENGLISH program to help crack.
2. Shift, Affine can try ALL keys.
3. Gen Sub, Keyword-Shift can crack: use Freq of n-grams, Hill-climbing.

Kerckhoff's principle

We made the comment **We KNOW that SHIFT was used.**
More generally we will always use the following assumption.
Kerckhoff's principle:

- Eve knows **The encryption scheme**.
- Eve knows **the alphabet and the language**.
- Eve does not know **the key**
- The key is chosen **at random**.

Vig and One-Time Pad and Psuedo-OTP

The Vigenère Cipher

Key: $k = (k_1, k_2, \ldots, k_n)$.
Encrypt (all arithmetic is mod 26)

$$Enc(m_1, m_2, \ldots, m_N) =$$

$$m_1 + k_1, m_2 + k_2, \ldots, m_n + k_n,$$

$$m_{n+1} + k_1, m_{n+2} + k_2, \ldots, m_{n+n} + k_n,$$

$$\ldots$$

Decrypt Decryption just reverses the process

Three Kinds of Vigenère Ciphers

1. Standard Vig: Use a longish-sentence. Key is Sentence.
2. Book Cipher: Use a book. Key is name of book and edition.
3. one-time pad: Key is randomly generated sequence.

Cracking Vig cipher

1. Find length of keyword either by spotting repeating patterns OR just try $L = 1, 2, 3, \ldots$ until you get it.
2. Given length L (which might not be right) divide text into L streams mod L and for each one guess shift and do IS-ENGLISH program
3. **Note** We use that taking every Lth letter of a text has same freq dist as normal English.

One-Time Pad

One-Time Pad

1. Let $\mathcal{M} = \{0, 1\}^n$, the set of all messages.

One-Time Pad

1. Let $\mathcal{M} = \{0, 1\}^n$, the set of all messages.

2. *Gen*: choose a uniform key $k \in \{0, 1\}^n$.

One-Time Pad

1. Let $\mathcal{M} = \{0,1\}^n$, the set of all messages.
2. *Gen*: choose a uniform key $k \in \{0,1\}^n$.
3. $Enc_k(m) = k \oplus m$.

One-Time Pad

1. Let $\mathcal{M} = \{0,1\}^n$, the set of all messages.
2. *Gen*: choose a uniform key $k \in \{0,1\}^n$.
3. $Enc_k(m) = k \oplus m$.
4. $Dec_k(c) = k \oplus c$.

One-Time Pad

1. **PRO** $\oplus$ is FAST!
2. **CON** If Key is N bits long can only send N bits.
3. **PRO** Uncrackable if use truly random bits.
4. **CON** Hard to get truly random bits.

Ways to Get Random-Looking Bits

1. **Linear Cong Gen** Pick x_0, A, B, M at random and then use:
   x_0
   $x_{i+1} = Ax_i + B \pmod{M}$
   CRACKABLE!- Some of you coded it up!
2. **Mersenne Twister** Also a recurrence, also crackable.
3. There are better methods used by NSA and others today.

The Matrix Cipher

Def Matrix Cipher. Pick M an $n \times n$ invertible over mod 26 matrix.

1. Encrypt via $xy \to M(xy)$.
2. Decrypt via $xy \to M^{-1}(xy)$.

Encode: Break text T into blocks of n, apply M to each block.

Decode: Do the same only with M^{-1}.

Matrix Cipher Crackable?

1. If n is small then crackable by brute force and IS-ENGLISH.
2. **Ciphertext Only Attack (COA)**. Brute force **looks like** it takes 26^{n^2}, but can get it down to $n26^n$. Still uncrackable but Alice and Bob need to up their n.
3. **Known Plaintext Attack (KPA)**. EASY to crack with linear algebra.

The History of Cryptography in One Slide

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).
2. Alice and Bob think its uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{64} matrices).

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).
2. Alice and Bob think its uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{64} matrices).
3. Eve Cracks it. (The trick above- only about 8×26^8.)

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).
2. Alice and Bob think its uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{64} matrices).
3. Eve Cracks it. (The trick above- only about 8×26^{8}.)
4. Lather, Rinse, Repeat.

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).
2. Alice and Bob think its uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{64} matrices).
3. Eve Cracks it. (The trick above- only about 8×26^8.)
4. Lather, Rinse, Repeat.

Above attack on Matrix Cipher is a microcosm of this history.

The History of Cryptography in One Slide

1. Alice and Bob come up with a Crypto system (e.g., Matrix Cipher with $n = 8$).
2. Alice and Bob think its uncrackable and have a "proof" that it is uncrackable (e.g., Eve HAS to go through all 26^{64} matrices).
3. Eve Cracks it. (The trick above- only about 8×26^8.)
4. Lather, Rinse, Repeat.

Above attack on Matrix Cipher is a microcosm of this history.

Proofs rely on limiting what Eve can do, and hence do not work if Eve does something else.

NY,NY Problem

Problem and Solution of our Ciphers/Terminology

1. Most of our ciphers are deterministic so always code m the same way. This leaks information.
2. One-Time Pad and Book Ciphers avoid this, but have very long keys.
3. The problem of the same message leading to the same ciphertext is called (by me)

   The NY,NY Problem.
4. If add randomization can avoid this problem. Randomized shift was an educational example, RSA was a real one.