BILL RECORDED LECTURE

REVIEW FOR FINAL

FINAL REVIEW-ADMIN

Final Review-Admin

1) Final is Friday Dec 18 1:30-3:30.

Final Review-Admin

1) Final is Friday Dec 18 1:30-3:30.

2) Will be at course website at 1:25 or so. Will be dealt with **just like a HW**.

Final Review-Admin

1) Final is Friday Dec 18 1:30-3:30.

2) Will be at course website at 1:25 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 18 1:30-3:30.

2) Will be at course website at 1:25 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 18 1:30-3:30.

2) Will be at course website at 1:25 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.

Final Review-Admin

1) Final is Friday Dec 18 1:30-3:30.

2) Will be at course website at 1:25 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.

6) We hope to grade it and post grades and final grades Friday Night.

Final Review-Admin

1) Final is Friday Dec 18 1:30-3:30.

2) Will be at course website at 1:25 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.

6) We hope to grade it and post grades and final grades Friday Night.

7) If can't take the exam OR have special circumstances tell me ASAP.

Final Review-Admin

1) Final is Friday Dec 18 1:30-3:30.

2) Will be at course website at 1:25 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.

6) We hope to grade it and post grades and final grades Friday Night.

7) If can't take the exam OR have special circumstances tell me ASAP.

8) Advice: Understand rather than memorize.

One-Letter Sub Ciphrs

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. Looks random?
5. Keyword-Mixed uses a word. Looks random?

1. All need IS-ENGLISH program to help crack.
2. Shift, Affine can try ALL keys.
3. Gen Sub, Keyword-X can crack: use Freq of n-grams, Hill-climbing.
4. There are ways to define **security**. 1-letter shift is secure.
5. There are ways to define **looks random**. Keyword-X do not.

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

How to Crack the Vig Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

How to Crack the Vig Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

Eve knows that (First Letter in Key) + (First Letter in Text) = 3.
Hence the following are the only possibilities for
(Letter in Key, Letter in Text) are:

(a, d), (z, e), (y, f), (w, g), $\ldots$, (b, c)

Only 26 possibilities. What of it? **Discuss**

How to Crack the Vig Book Cipher

Eve sees a d. (Recall that $d = 3$.) What does Eve know? **Discuss**

Eve knows that (First Letter in Key) + (First Letter in Text) = 3.
Hence the following are the only possibilities for
(Letter in Key, Letter in Text) are:

(a, d), (z, e), (y, f), (w, g), $\ldots$, (b, c)

Only 26 possibilities. What of it? **Discuss**
Some of the pairs are more likely than others.

1. **Both** the key **and** the text are in English.
2. (z, e): Hmm, z is unlikely but e is likely.
3. (a, d): Hmm, seems more likely than (z, e).
4. Can rank which are more likely (e.g., add or mult the freqs).
5. Can then use adjacent letters and freq of adjacent pairs, and rank them.
6. Triples. Etc.

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. **Merseen Twister** Also a recurrence, also crackable.
3. **VN method** if can generate bits with prob(0)=p, prob(1)=$1-p$ can use to get truly random bits without knowing p.
   Takes a long time to get the bits.
   Generating bits with prob p, $1-p$, still hard.
4. There are better methods used by NSA and others today.

Cracking Linear Cong Gen

1. Have some word or phrase that you think is there. E.g., **PAKISTAN.** Say its 8 letters.
2. For EVERY 8-letter block (until you succeed) do the thought experliement: What if its **PAKISTAN**?
   - 2.1 Based on that guess find equations that relate A, B, M.
   - 2.2 Try to solve those equations. If no solution goto next block-of-8.
   - 2.3 There is ≥ 1 solution (A, B, M). Use it to find x_0 and the entire plaintext T.
   - 2.4 Test if T IS-English. If so then DONE. If not then goto next block-of-8.

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 uncracble 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.

Misc Ciphers

Misc Ciphers

1. Playfair Cipher: A compact way to sub 2-letter blocks. Keyspace to small in modern era.
2. Rail Fence Cipher: Might work if do not believe Kerchoff's Principle.
3. Autokey: Very good if you do not believe Kerchoff's principle.
4. Book Cipher (diff definition that when used with Vig) where you both have books and refer to words in it. Known to be crackable, but takes some effort. If Alice and Bob are muffin-mathematicians they **should not** use **Mathematical Muffin Morsels**.

Misc Ciphers

1. Playfair Cipher: A compact way to sub 2-letter blocks. Keyspace to small in modern era.
2. Rail Fence Cipher: Might work if do not believe Kerchoff's Principle.
3. Autokey: Very good if you do not believe Kerchoff's principle.
4. Book Cipher (diff definition that when used with Vig) where you both have books and refer to words in it. Known to be crackable, but takes some effort. If Alice and Bob are muffin-mathematicians they **should not** use **Mathematical Muffin Morsels**. Too bad- I could use more sales. Amazon Rank is around 3,000,000.

NY,NY Problem

A Problem with MOST 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.

How to Fix This Without a Long Key

Randomized Shift Key is a **function** $f : S \to S$.

1. To send message $(m_1, \ldots, m_L)$ (each m_i is a character):
   - 1.1 Pick random $r_1, \ldots, r_L \in S$.
   - 1.2 Send $((r_1; m_1 + f(r_1)), \ldots, (r_L; m_L + f(r_L)))$.

How to Fix This Without a Long Key

Randomized Shift Key is a **function** $f : S \to S$.

1. To send message $(m_1, \ldots, m_L)$ (each m_i is a character):
   1.1 Pick random $r_1, \ldots, r_L \in S$.
   1.2 Send $((r_1; m_1 + f(r_1)), \ldots, (r_L; m_L + f(r_L)))$.
2. To decode message $((r_1; c_1), \ldots, (r_L; c_L))$:
   2.1 Find $(c_1 - f(r_1), \ldots, c_L - f(r_L))$.

This cipher is crackable but gives the idea for how to fix ciphers to avoid NY,NY problem.

Summary of the NY,NY Problem and Solution

Summary of the NY,NY Problem and Solution

1. Det. Ciphers: Message M always maps to the same thing. Boo!

Summary of the NY,NY Problem and Solution

1. Det. Ciphers: Message M always maps to the same thing. Boo!
2. We can turn any Det. Cipher into a randomized one. Will use this later in the course.

Summary of the NY,NY Problem and Solution

1. Det. Ciphers: Message M always maps to the same thing. Boo!
2. We can turn any Det. Cipher into a randomized one. Will use this later in the course.
3. If turn a weak Det. Cipher (like Shift) into a randomized one, still crackable.

Summary of the NY,NY Problem and Solution

1. Det. Ciphers: Message M always maps to the same thing. Boo!
2. We can turn any Det. Cipher into a randomized one. Will use this later in the course.
3. If turn a weak Det. Cipher (like Shift) into a randomized one, still crackable.
4. Cracking it takes a much longer text.