Something Wrong With All Cipher So Far

Lecture 05

Even Short Messages Insecure

Let C be any of Shift, Affine, Vigenere, Matrix.
Recall: C is crackable if text is long enough.

Even Short Messages Insecure

Let C be any of Shift, Affine, Vigenere, Matrix.
Recall: C is crackable if text is long enough.

What About Short Messages?: discuss

Even Short Messages Insecure

Let C be any of Shift, Affine, Vigenere, Matrix.
Recall: C is crackable if text is long enough.

What About Short Messages?: discuss

Recall: For Shift Eve can tell if two messages same or not.

Even Short Messages Insecure

Let C be any of Shift, Affine, Vigenere, Matrix.
Recall: C is crackable if text is long enough.

What About Short Messages?: discuss

Recall: For Shift Eve can tell if two messages same or not.

Not Just Shift: For C Eve can tell if two messages same or not.

Even Short Messages Insecure

Let C be any of Shift, Affine, Vigenere, Matrix.
Recall: C is crackable if text is long enough.

What About Short Messages?: discuss

Recall: For Shift Eve can tell if two messages same or not.

Not Just Shift: For C Eve can tell if two messages same or not.

Danger! Eve knows the message will say where spy is. Will be of the form city,state (without punctuation).

Even Short Messages Insecure

Let C be any of Shift, Affine, Vigenere, Matrix.
Recall: C is crackable if text is long enough.

What About Short Messages?: discuss

Recall: For Shift Eve can tell if two messages same or not.

Not Just Shift: For C Eve can tell if two messages same or not.

Danger! Eve knows the message will say where spy is. Will be of the form city,state (without punctuation).
Alice sends to Bob adecn aapad ecnaa pxuaq.

Even Short Messages Insecure

Let C be any of Shift, Affine, Vigenere, Matrix.
Recall: C is crackable if text is long enough.

What About Short Messages?: discuss

Recall: For Shift Eve can tell if two messages same or not.

Not Just Shift: For C Eve can tell if two messages same or not.

Danger! Eve knows the message will say where spy is. Will be of the form city,state (without punctuation).
Alice sends to Bob adecn aapad ecnaa pxuaq.
Eve notices adecnaap adecnaap xuaq.

Even Short Messages Insecure

Let C be any of Shift, Affine, Vigenere, Matrix.
Recall: C is crackable if text is long enough.

What About Short Messages?: discuss

Recall: For Shift Eve can tell if two messages same or not.

Not Just Shift: For C Eve can tell if two messages same or not.

Danger! Eve knows the message will say where spy is. Will be of the form city,state (without punctuation).
Alice sends to Bob adecn aapad ecnaa pxuaq.
Eve notices adecnaap adecnaap xuaq.
Even knows that the city and state are the same!

What Does Eve Know?

Cities with states name. * means no longer a city.

What Does Eve Know?

Cities with states name. * means no longer a city.

Alabama*, Arizona*, Arkansas, California, Colorado*, Delaware, Florida, New Georgia*, Idaho, Illinois*, Indianapolis, Iowa, Jersey, Kansas, Maryland*, Minneapolis, Minnesota, Mississippi*, Missouri, Montana, Nebraska, Nevada*, New York, Ohio, Oklahoma, Oregon, Tennessee*, Texas, Utah*, Virginia*, Virginia Beach, Wisconsin Dells, Wisconsin Rapids.

What Does Eve Know?

Cities with states name. * means no longer a city.

Alabama*, Arizona*, Arkansas, California, Colorado*, Delaware, Florida, New Georgia*, Idaho, Illinois*, Indianapolis, Iowa, Jersey, Kansas, Maryland*, Minneapolis, Minnesota, Mississippi*, Missouri, Montana, Nebraska, Nevada*, New York, Ohio, Oklahoma, Oregon, Tennessee*, Texas, Utah*, Virginia*, Virginia Beach, Wisconsin Dells, Wisconsin Rapids.

There are 33 such cities, 22 of which still exist.
Eve's search for the spy is reduced!

How to Fix This?

Problem: If C is any of the ciphers discussed then Eve can tell when two messages are the same.

Discuss: Is there a cipher for which Eve cannot tell this?

How to Fix This?

Problem: If C is any of the ciphers discussed then Eve can tell when two messages are the same.

Discuss: Is there a cipher for which Eve cannot tell this?
Need that even if $x = y$ could have $C(x) \neq C(y)$.

Discuss: How can we do that?

How to Fix This?

Problem: If C is any of the ciphers discussed then Eve can tell when two messages are the same.

Discuss: Is there a cipher for which Eve cannot tell this?
Need that even if $x = y$ could have $C(x) \neq C(y)$.

Discuss: How can we do that?

Use a very long key and keep using different parts of it.
This is the idea behind 1-time pad which we study soon.

How to Fix This?

Problem: If C is any of the ciphers discussed then Eve can tell when two messages are the same.

Discuss: Is there a cipher for which Eve cannot tell this?
Need that even if $x = y$ could have $C(x) \neq C(y)$.

Discuss: How can we do that?

Use a very long key and keep using different parts of it.
This is the idea behind 1-time pad which we study soon.

Discuss: Can we do this without a long key?

How to Fix This Without a Long Key

Obstacle: All of our ciphers are deterministic. Need Rand.

How to Fix This Without a Long Key

Obstacle: All of our ciphers are deterministic. Need Rand.
Recall Deterministic Shift: Key is $s \in S$.

1. To send message $(m_1, \ldots, m_L)$ send $(m_1 + s, \ldots, m_L + s)$
2. To decode message $(c_1, \ldots, c_L)$ find $(c_1 - s, \ldots, c_L - s)$

How to Fix This Without a Long Key

Obstacle: All of our ciphers are deterministic. Need Rand.
Recall Deterministic Shift: Key is $s \in S$.

1. To send message $(m_1, \ldots, m_L)$ send $(m_1 + s, \ldots, m_L + s)$
2. To decode message $(c_1, \ldots, c_L)$ find $(c_1 - s, \ldots, c_L - s)$

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 $r_1, \ldots, r_L \in S$. For $1 \le i \le L$ compute $s_i = f(r_i)$.
   - 1.2 Send $((r_1; m_1 + s_1), \ldots, (r_L; m_L + s_L))$
2. To decode message $((r_1; c_1), \ldots, (r_L; c_L))$
   - 2.1 For $1 \le i \le L$ $s_i = f(r_i)$.
   - 2.2 Find $(c_1 - s_1, \ldots, c_L - s_L)$

Example

The key is $f(r) = 2r + 7$. Alice wants to send NY,NY which we interpret as nyny.
Need four shifts.

Pick random $r = 4$, so first shift is $2 * 4 + 7 = 15$
Pick random $r = 10$, so second shift is $2 * 10 + 7 = 1$
Pick random $r = 1$, so third shift is $2 * 1 + 7 = 9$
Pick random $r = 17$, so fourth shift is $2 * 17 + 7 = 15$

Send (4;C), (10,Z), (1,W), (17,N)

Eve will not be able to tell that is of the form XYXY.

PROS and CONS of Randomized Shift

Discuss

PROS and CONS of Randomized Shift

Discuss

PRO: If Alice sends NY,NY Eve can't tell its XYXY.

PROS and CONS of Randomized Shift

Discuss

PRO: If Alice sends NY,NY Eve can't tell its XYXY.

PRO: More generally, Eve cannot tell if two messages are the same.

PROS and CONS of Randomized Shift

Discuss
PRO: If Alice sends NY,NY Eve can't tell its XYXY.
PRO: More generally, Eve cannot tell if two messages are the same.
CON: More effort on Alice and Bob's part.

PROS and CONS of Randomized Shift

Discuss

PRO: If Alice sends NY,NY Eve can't tell its XYXY.

PRO: More generally, Eve cannot tell if two messages are the same.

CON: More effort on Alice and Bob's part.

Question: Is Randomized Shift crackable? Discuss.

Cracking Randomized Shift

With a long text Rand Shift is crackable.
If N is long and Eve sees

$$(r_1; \sigma_1)(r_2; \sigma_2) \cdots (r_N; \sigma_N)$$

Then many r will appear many times. Say r appears 10,000 times. then Eve knows the shift of lots of letters.

1. From our study of Vig we know that every Lth letter has same freq dist as English.
2. It turns out that if you take RANDOM letters, also get same freq dist as English

Hence can find $f(r)$. If do this for many r, have f.

Cracking Randomized Shift

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting two same is $\geq p$.

If pick m then
1) number of ways is n^m
2) number of ways they are all diff is $\sim n(n-1)\cdots(n-m)$
Prob of all diff is

$$\frac{n(n-1)\cdots(n-m)}{n^m} = \frac{n-1}{n} \times \frac{n-2}{n} \cdots \frac{n-m}{n}$$

$$= \left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) \cdots \left(1 - \frac{m}{n}\right) \sim e^{-1/n-2/n-\cdots-m/n}$$

$$= e^{-\frac{1}{n}(1+2+\cdots+m)} \sim e^{-\frac{m(m+1)}{2n}} \sim e^{-\frac{m^2}{2n}}$$

Cracking Randomized Shift

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting two same is $\geq p$.

m must satisfy $e^{-\frac{m^2}{2n}} \leq 1 - p$. Try $m = \sqrt{an}$

$$e^{-\frac{m^2}{n}} = e^{-a} < 1 - p$$

Need $a > -\ln(1-p)$. Example: if $p = .99$ then need $a \geq 5$ suffices.

Note: Need only wait $\sim \sqrt{n}$ for a repeat. This is important for Randomized Shift. Will also use later in course

Upshot: After $\sqrt{an}$ numbers prob have a repeat. a is small.

Cracking Randomized Shift

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting 2 of the same is ≥ 0.9.

Cracking Randomized Shift

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting 2 of the same is ≥ 0.9. $m = O(n^{1/2})$.

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting 3 of the same is ≥ 0.9.

Cracking Randomized Shift

Question: Pick numbers from $\{1,\ldots,n\}$ rand. Want m so if pick m, prob of getting 2 of the same is ≥ 0.9. $m = O(n^{1/2})$.
Question: Pick numbers from $\{1,\ldots,n\}$ rand. Want m so if pick m, prob of getting 3 of the same is ≥ 0.9. $m = O(n^{2/3})$.
Question: Pick numbers from $\{1,\ldots,n\}$ rand. Want m so if pick m, prob of getting 4 of the same is ≥ 0.9.

Cracking Randomized Shift

Question: Pick numbers from $\{1,\ldots,n\}$ rand. Want m so if pick m, prob of getting 2 of the same is ≥ 0.9. $m = O(n^{1/2})$.
Question: Pick numbers from $\{1,\ldots,n\}$ rand. Want m so if pick m, prob of getting 3 of the same is ≥ 0.9. $m = O(n^{2/3})$.
Question: Pick numbers from $\{1,\ldots,n\}$ rand. Want m so if pick m, prob of getting 4 of the same is ≥ 0.9. $m = O(n^{3/4})$.
Question: Pick numbers from $\{1,\ldots,n\}$ rand. Want m so if pick m, prob of getting a of the same is ≥ 0.9.

Cracking Randomized Shift

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting 2 of the same is ≥ 0.9. $m = O(n^{1/2})$.

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting 3 of the same is ≥ 0.9. $m = O(n^{2/3})$.

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting 4 of the same is ≥ 0.9. $m = O(n^{3/4})$.

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting a of the same is ≥ 0.9. $m = O(n^{1-(1/a)})$.

Proof of the above:

Cracking Randomized Shift

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting 2 of the same is ≥ 0.9. $m = O(n^{1/2})$.

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting 3 of the same is ≥ 0.9. $m = O(n^{2/3})$.

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting 4 of the same is ≥ 0.9. $m = O(n^{3/4})$.

Question: Pick numbers from $\{1, \ldots, n\}$ rand. Want m so if pick m, prob of getting a of the same is ≥ 0.9. $m = O(n^{1-(1/a)})$.

Proof of the above: Arvind Srinivasan told me and he is expert on probabiity.

Upshot: Can get repeats fairly often. Can use this to find $f(0)$, $f(1)$, etc, $f(25)$.

Origin of Randomized Shift

I made it up for this course to make a point about sending the same message twice.

The point I am making is very important! Eve should NOT be able to tell that two messages are the same. This is a real issue in crypto that I expressed in a fake way.

The One-Time Pad

Lecture 05

One-time pad

- Patented in 1917 by Vernam
  - Recent historical research indicates it was invented (at least) 35 years earlier

One-time pad

- Let $\mathcal{M} = \{0,1\}^n$
- *Gen*: choose a uniform key $k \in \{0,1\}^n$
- $Enc_k(m) = k \oplus m$
- $Dec_k(c) = k \oplus c$
- Correctness:

$$\begin{aligned} Dec_k(Enc_k(m)) &= k \oplus (k \oplus m) \\ &= (k \oplus k) \oplus m \\ &= m \end{aligned}$$

Example Of One-time pad

Key is 10001010001000111110111100
Alice wants to send Bob 1110.
She sends $1110 \oplus 1000 = 0110$
Then Bob wants to send Alice 00111.
He sends $00111 \oplus 10100 = 10011$.

1. If Key is N bits long can only send N bits.
2. $\oplus$ is FAST!

Example Of One-time pad

Key is 10001010001000111110111100
Alice wants to send Bob 1110.
She sends $1110 \oplus 1000 = 0110$
Then Bob wants to send Alice 00111.
He sends $00111 \oplus 10100 = 10011$.

1. If Key is N bits long can only send N bits.
2. $\oplus$ is FAST!

Is the one-time pad uncrackable:
VOTE: Yes, No, or Other.

Example Of One-time pad

Key is 10001010001000111110111100

Alice wants to send Bob 1110.

She sends $1110 \oplus 1000 = 0110$

Then Bob wants to send Alice 00111.

He sends $00111 \oplus 10100 = 10011$.

1. If Key is N bits long can only send N bits.
2. $\oplus$ is FAST!

Is the one-time pad uncrackable:

VOTE: Yes, No, or Other.

Yes. Really!

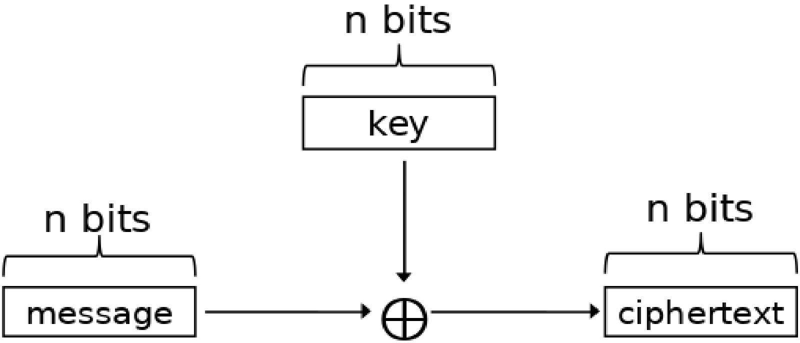
Example Of One-time pad

Key is 10001010001000111110111100
Alice wants to send Bob 1110.
She sends $1110 \oplus 1000 = 0110$
Then Bob wants to send Alice 00111.
He sends $00111 \oplus 10100 = 10011$.

1. If Key is N bits long can only send N bits.
2. $\oplus$ is FAST!

Is the one-time pad uncrackable:
VOTE: Yes, No, or Other.
Yes. Really!
Caveat: Generating truly random bits is hard.

One-time pad



Something ELSE Wrong With All Cipher So Far

Lecture 05

Eve Can Tamper with Message

1. Eve knows that Alice is going to send Bob a number that is < 999 which indicates how much money Bob should give Eve.
2. They will send in binary using use one-time-pad.
3. Alice sends the message 1001101010010110.
4. Eve intercepts and tampers with msg before Bob gets it.
5. Can Eve tamper with it in a way that matters? Discuss

Yes: Eve Knows the 10th bit of real message is 0 since she gets $999 < 1024$ dollars. Let b be the 10th bit that is send. Eve Flips 10th Bit in ciphtext to flip 10th bit in numbers

Original Message:	1001101010010110
Eve Tampers:	1001101000010110

Eve just got 1024 more dollars!

Lesson Learned/Our Goal

Security: Eve cannot learn message

Integrity: Bob can be sure the message came from Alice

Lesson Learned: One-time-pad is Secure but lacks integrity. Security does not imply integrity.

Question: Does Integrity imply Security. Discuss

Lesson Learned/Our Goal

Security: Eve cannot learn message

Integrity: Bob can be sure the message came from Alice

Lesson Learned: One-time-pad is Secure but lacks integrity.
Security does not imply integrity.

Question: Does Integrity imply Security.Discuss

No. Will discuss later.

Goal for now: Make Shift Cipher not forgeable.
Discuss

Has No Name (HNN) Shift

HNN shift: Key is a shift s and a function $g : S \rightarrow S$.

1. To send message $(m_1, \ldots, m_L)$ (each m_i is a char) send

$$(m_1 + s, g(m_1)), \ldots, (m_L + s, g(m_L)).$$

2. To decode message $((c_1, d_1), \ldots, (c_L, d_L))$ just

$$(c_1 - s, \ldots, c_L - s).$$

3. To authenticate Once Bob has $m_1, \ldots, m_L$ he computes $g(m_1), \ldots, g(m_L)$ and checks that, for all i, $g(m_i) = d_i$.