

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

When Hackers Attack!

September 28, 2020

Ciphertext and Plaintext

Plaintext The message Alice really wants to send to Bob, e.g.
Meet me after class.

Ciphertext and Plaintext

Plaintext The message Alice really wants to send to Bob, e.g.
Meet me after class.

Ciphertext What Alice sends Bob. The hope is that if Eve sees it she will **not** learn the plaintext. E.g.

PHHWP HDIWH UFODV V

Types of Attacks

We will describe several different types of attacks Eve can use.
They depend on:

1. What information Eve has access to.
2. What computing power Eve has.

Types of Attacks

We will describe several different types of attacks Eve can use.
They depend on:

1. What information Eve has access to.
2. What computing power Eve has.

Eve's goal is to find out something about the plaintext she did not already know.

Ciphertext Only Attack (COA)

Ciphertext Only Attacks (COA) All Eve has is the ciphertext.

Ciphertext Only Attack (COA)

Ciphertext Only Attacks (COA) All Eve has is the ciphertext.
Eve cracked shift, affine, general sub, Vig with a COA.

Known Plaintext Attack (KPA)

Known Plaintext Attack (KPA) Eve knows the plaintext for **some of** the ciphertext.

Known Plaintext Attack (KPA)

Known Plaintext Attack (KPA) Eve knows the plaintext for **some of** the ciphertext.

Eve can crack Matrix and Linear-Cong-Gen ciphers with a KPA.

Known Plaintext Attack (KPA)

Known Plaintext Attack (KPA) Eve knows the plaintext for **some of** the ciphertext.

Eve can crack Matrix and Linear-Cong-Gen ciphers with a KPA.
How can Eve obtain plaintext for some of the ciphertext?

Known Plaintext Attack (KPA)

Known Plaintext Attack (KPA) Eve knows the plaintext for **some of** the ciphertext.

Eve can crack Matrix and Linear-Cong-Gen ciphers with a KPA. How can Eve obtain plaintext for some of the ciphertext?

1. If yesterday the message **ABC DEFG** was where the spy would be, and today Eve found the spy in **New York**, then **ABC DEFG** decodes to **New York**.

Known Plaintext Attack (KPA)

Known Plaintext Attack (KPA) Eve knows the plaintext for **some of** the ciphertext.

Eve can crack Matrix and Linear-Cong-Gen ciphers with a KPA. How can Eve obtain plaintext for some of the ciphertext?

1. If yesterday the message **ABC DEFG** was where the spy would be, and today Eve found the spy in **New York**, then **ABC DEFG** decodes to **New York**.
2. **WWII History** A German soldier in an area where nothing was happening sent **nothing to report** every day.

Known Plaintext Attack (KPA)

Known Plaintext Attack (KPA) Eve knows the plaintext for **some of** the ciphertext.

Eve can crack Matrix and Linear-Cong-Gen ciphers with a KPA. How can Eve obtain plaintext for some of the ciphertext?

1. If yesterday the message **ABC DEFG** was where the spy would be, and today Eve found the spy in **New York**, then **ABC DEFG** decodes to **New York**.
2. **WWII History** A German soldier in an area where nothing was happening sent **nothing to report** every day.
3. Guess a word that you think appears in the document. For Linear-Cong-Gen our example was **Pakistan**.

Known Plaintext Attack (KPA)

Known Plaintext Attack (KPA) Eve knows the plaintext for **some of** the ciphertext.

Eve can crack Matrix and Linear-Cong-Gen ciphers with a KPA. How can Eve obtain plaintext for some of the ciphertext?

1. If yesterday the message **ABC DEFG** was where the spy would be, and today Eve found the spy in **New York**, then **ABC DEFG** decodes to **New York**.
2. **WWII History** A German soldier in an area where nothing was happening sent **nothing to report** every day.
3. Guess a word that you think appears in the document. For Linear-Cong-Gen our example was **Pakistan**.
4. **More WWII History** Turing and his gang cracked the German Enigma Code, guessing that **ein** (German for **one**) would be in messages.

Chosen Plaintext Attack (CPA)

Chosen Plaintext Attack (CPA) Eve tricks Alice into encoding a particular plaintext.

Chosen Plaintext Attack (CPA)

Chosen Plaintext Attack (CPA) Eve tricks Alice into encoding a particular plaintext.

Later in the course we will see a CPA attack on RSA.

Chosen Plaintext Attack (CPA)

Chosen Plaintext Attack (CPA) Eve tricks Alice into encoding a particular plaintext.

Later in the course we will see a CPA attack on RSA.

1. **WWII History** America thought that the Japanese code for Midway was **AF**. So the Americans send the message to a ship **Midway is low on supplies**. The Americans observe that the next Japanese message has **AF** in it, so their suspicions are confirmed.

Chosen Plaintext Attack (CPA)

Chosen Plaintext Attack (CPA) Eve tricks Alice into encoding a particular plaintext.

Later in the course we will see a CPA attack on RSA.

1. **WWII History** America thought that the Japanese code for Midway was **AF**. So the Americans send the message to a ship **Midway is low on supplies**. The Americans observe that the next Japanese message has **AF** in it, so their suspicions are confirmed.
2. **WWII History** England put mines in places that the Germans had no abbreviations for. The Germans cleared those mines and send **NAME OF PLACE, all clear**, transmitted in code.

Chosen Ciphertext Attack (CCA)

Chosen Ciphertext Attack (CCA) Eve tricks Alice into decoding a particular ciphertext.

Chosen Ciphertext Attack (CCA)

Chosen Ciphertext Attack (CCA) Eve tricks Alice into decoding a particular ciphertext.

Later in the course we may see a CCA attack on RSA.

Dictionary Attack

Dictionary Attack Many variants, we give two:

1. Have database of **X** decodes to **Y** and pattern match.
2. Use Dictionary to guess passwords.

Dictionary Attack

Dictionary Attack Many variants, we give two:

1. Have database of **X** decodes to **Y** and pattern match.
2. Use Dictionary to guess passwords. Or guess on of the most common passwords:

Dictionary Attack

Dictionary Attack Many variants, we give two:

1. Have database of **X** decodes to **Y** and pattern match.
2. Use Dictionary to guess passwords. Or guess on of the most common passwords:

123456	<i>Password</i>	12345678	<i>qwerty</i>	12345
12345678	<i>letmein</i>	1234567	<i>football</i>	<i>iloveyou</i>
<i>admin</i>	<i>welcome</i>	<i>monkey</i>	<i>login</i>	<i>abc123</i>
<i>starwars</i>	123123	<i>dragon</i>	<i>passwOrd</i>	<i>master</i>
<i>hello</i>	<i>freedom</i>	<i>whatever</i>	<i>qazwsx</i>	<i>trusno1</i>

Dictionary Attack

Dictionary Attack Many variants, we give two:

1. Have database of **X** decodes to **Y** and pattern match.
2. Use Dictionary to guess passwords. Or guess on of the most common passwords:

123456	<i>Password</i>	12345678	<i>qwerty</i>	12345
12345678	<i>letmein</i>	1234567	<i>football</i>	<i>iloveyou</i>
<i>admin</i>	<i>welcome</i>	<i>monkey</i>	<i>login</i>	<i>abc123</i>
<i>starwars</i>	123123	<i>dragon</i>	<i>passwOrd</i>	<i>master</i>
<i>hello</i>	<i>freedom</i>	<i>whatever</i>	<i>qazwsx</i>	<i>trusno1</i>

qwerty: 1st 6 letters on 3rd line of a keyboard.

qazwsz: Similar keyboard shenanigans.

Dictionary Attack

Dictionary Attack Many variants, we give two:

1. Have database of **X** decodes to **Y** and pattern match.
2. Use Dictionary to guess passwords. Or guess on of the most common passwords:

123456	<i>Password</i>	12345678	<i>qwerty</i>	12345
12345678	<i>letmein</i>	1234567	<i>football</i>	<i>iloveyou</i>
<i>admin</i>	<i>welcome</i>	<i>monkey</i>	<i>login</i>	<i>abc123</i>
<i>starwars</i>	123123	<i>dragon</i>	<i>passwOrd</i>	<i>master</i>
<i>hello</i>	<i>freedom</i>	<i>whatever</i>	<i>qazwsx</i>	<i>trusno1</i>

qwerty: 1st 6 letters on 3rd line of a keyboard.

qazwsz: Similar keyboard shenanigans.

trusno1: I like that one, I think I'll use it :-)

Brute Force Attacks (BFA)

Brute Force Attacks (BFA) Guess all possible keys.

Brute Force Attacks (BFA)

Brute Force Attacks (BFA) Guess all possible keys.
We cracked shift, affine, Vig, this way.

Brute Force Attacks (BFA)

Brute Force Attacks (BFA) Guess all possible keys.

We cracked shift, affine, Vig, this way.

Only effective if either:

Brute Force Attacks (BFA)

Brute Force Attacks (BFA) Guess all possible keys.

We cracked shift, affine, Vig, this way.

Only effective if either:

1. The key space is small enough for Eve's computing power.

Brute Force Attacks (BFA)

Brute Force Attacks (BFA) Guess all possible keys.

We cracked shift, affine, Vig, this way.

Only effective if either:

1. The key space is small enough for Eve's computing power.
2. Some cleverness can cut down the key space before you do BFA.

Brute Force Attacks (BFA)

Brute Force Attacks (BFA) Guess all possible keys.

We cracked shift, affine, Vig, this way.

Only effective if either:

1. The key space is small enough for Eve's computing power.
2. Some cleverness can cut down the key space before you do BFA.

Easy to thwart Use a bigger key space!

Timing and Power Attacks

Use how much time or power a cryptosystem is using to figure out information about the key and narrow down the keyspace.

Timing and Power Attacks

Use how much time or power a cryptosystem is using to figure out information about the key and narrow down the keyspace.

1. Scary!

Timing and Power Attacks

Use how much time or power a cryptosystem is using to figure out information about the key and narrow down the keyspace.

1. Scary! Alice and Bob are using cryptosystem C such that Eve can crack C with a CPA attack iff Eve can Solve the ERIC problem.

Timing and Power Attacks

Use how much time or power a cryptosystem is using to figure out information about the key and narrow down the keyspace.

1. Scary! Alice and Bob are using cryptosystem C such that Eve can crack C with a CPA attack iff Eve can Solve the ERIC problem. The mathematical proof of this does not take timing attacks into account.

Timing and Power Attacks

Use how much time or power a cryptosystem is using to figure out information about the key and narrow down the keyspace.

1. Scary! Alice and Bob are using cryptosystem C such that Eve can crack C with a CPA attack iff Eve can Solve the ERIC problem. The mathematical proof of this does not take timing attacks into account.

Alice and Bob can easily thwart timing/power attacks by padding. But there was a time before this attack was known when it may have been effective.

Timing and Power Attacks

Use how much time or power a cryptosystem is using to figure out information about the key and narrow down the keyspace.

1. Scary! Alice and Bob are using cryptosystem C such that Eve can crack C with a CPA attack iff Eve can Solve the ERIC problem. The mathematical proof of this does not take timing attacks into account.

Alice and Bob can easily thwart timing/power attacks by padding. But there was a time before this attack was known when it may have been effective.

2. There may be other attacks that we do not know about like Timing/Power was. It may be hard (impossible?) to prove that there is no such attack that works. This involves issues outside of the Mathematical realm.

Timing and Power Attacks

Use how much time or power a cryptosystem is using to figure out information about the key and narrow down the keyspace.

1. Scary! Alice and Bob are using cryptosystem C such that Eve can crack C with a CPA attack iff Eve can Solve the ERIC problem. The mathematical proof of this does not take timing attacks into account.

Alice and Bob can easily thwart timing/power attacks by padding. But there was a time before this attack was known when it may have been effective.

2. There may be other attacks that we do not know about like Timing/Power was. It may be hard (impossible?) to prove that there is no such attack that works. This involves issues outside of the Mathematical realm.
3. Look up the Maginot Line.

Examples of Timing Attacks

Examples of Timing Attacks

1. **Spectre** A vulnerability that affects modern microprocessors that perform branch prediction (guessing which branch of a future IF statement will be executed, and executing it ahead of time to save time).

`https://en.wikipedia.org/wiki/Spectre_\(security_vulnerability\)`

Examples of Timing Attacks

1. **Spectre** A vulnerability that affects modern microprocessors that perform branch prediction (guessing which branch of a future IF statement will be executed, and executing it ahead of time to save time).
[https://en.wikipedia.org/wiki/Spectre_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Spectre_(security_vulnerability))
2. **Meltdown** A Hardware vulnerability affecting X86 microprocessors, IBM POWER processors, and some others.
[https://en.wikipedia.org/wiki/Meltdown_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability))

Examples of Timing Attacks

1. **Spectre** A vulnerability that affects modern microprocessors that perform branch prediction (guessing which branch of a future IF statement will be executed, and executing it ahead of time to save time).
[https://en.wikipedia.org/wiki/Spectre_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Spectre_(security_vulnerability))
2. **Meltdown** A Hardware vulnerability affecting X86 microprocessors, IBM POWER processors, and some others.
[https://en.wikipedia.org/wiki/Meltdown_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability))
3. **Attack on RSA** Will cover this later.

Are Timing/Power Attacks Our Concern?

This course will not deal with preventing Timing/Power attacks.

Are Timing/Power Attacks Our Concern?

This course will not deal with preventing Timing/Power attacks.
So then why did I mention them?

Are Timing/Power Attacks Our Concern?

This course will not deal with preventing Timing/Power attacks.
So then why did I mention them?

1. Make the point that Security (CMSC 414) is an important partner to Crypto.

Are Timing/Power Attacks Our Concern?

This course will not deal with preventing Timing/Power attacks.
So then why did I mention them?

1. Make the point that Security (CMSC 414) is an important partner to Crypto.
2. My own fascination with the concept. I normally teach and work in:

Are Timing/Power Attacks Our Concern?

This course will not deal with preventing Timing/Power attacks.
So then why did I mention them?

1. Make the point that Security (CMSC 414) is an important partner to Crypto.
2. My own fascination with the concept. I normally teach and work in:
 - 2.1 **Discrete Math** No claim to real world applications.

Are Timing/Power Attacks Our Concern?

This course will not deal with preventing Timing/Power attacks.
So then why did I mention them?

1. Make the point that Security (CMSC 414) is an important partner to Crypto.
2. My own fascination with the concept. I normally teach and work in:
 - 2.1 **Discrete Math** No claim to real world applications.
 - 2.2 **Elementary Theory of Comp** Mostly theoretical.

Are Timing/Power Attacks Our Concern?

This course will not deal with preventing Timing/Power attacks.
So then why did I mention them?

1. Make the point that Security (CMSC 414) is an important partner to Crypto.
2. My own fascination with the concept. I normally teach and work in:
 - 2.1 **Discrete Math** No claim to real world applications.
 - 2.2 **Elementary Theory of Comp** Mostly theoretical.
 - 2.3 **Ramsey Theory and its “Applications”** Need I say more?

Are Timing/Power Attacks Our Concern?

This course will not deal with preventing Timing/Power attacks.
So then why did I mention them?

1. Make the point that Security (CMSC 414) is an important partner to Crypto.
2. My own fascination with the concept. I normally teach and work in:
 - 2.1 **Discrete Math** No claim to real world applications.
 - 2.2 **Elementary Theory of Comp** Mostly theoretical.
 - 2.3 **Ramsey Theory and its “Applications”** Need I say more?
 - 2.4 Hence teaching this course is a real eye-opener in that it **really applies** to the real world and hence its fascinating and frustrating to see what it can and cannot do.