An invitation to

Modern Cryptography

Mihir Bellare
UCSD

I like Cryptography because it is

Fascinating
and
Useful

Cool ideas
Pretty math
Philosophy made precise

Cyber shopping
Electronic banking
Bitcoin
Tor

But what IS “Cryptography”? 

How many can you name?

There is no such thing as Art, really.
There are only ARTISTS.

The Story of Art
E. H. Gombrich

There is no such thing as Art, really.
There are only ARTISTS.

The Story of Art
E. H. Gombrich
There is no such thing as Cryptography, really.
There are only CRYPTOGRAPHERS.

How many can you name?

This course is a series of short stories
about what cryptographers do
and how they see the world.

Cryptography is ALIVE.
Not a textbook.

Cryptography is SOCIALLY CONSTRUCTED.

There is no such thing as Cryptography, really.
There are only CRYPTOGRAPHERS.

How many have won the TURING AWARD?

A grey slide like THIS represents the END of a SEGMENT.

To take a BREATH.

And DISCUSS!

What does it mean to say that there is no such thing as art / cryptography, really; there are only artists / cryptographers?

What does it mean to say that a discipline is socially constructed?
Security GOALS, ADVERSARIES, and the Security MINDSET

Security Goals

PRIVACY  AUTHENTICITY  IDENTITY  ...

I don’t want others to see my emails or chats; get my social-security number, credit-card number or medical records; know which web sites I visit, what I buy, where I travel. I don’t want them to know my salary, how I vote, what movies I like, whether I sing in the shower.

Coca-Cola does not want its formula revealed, corporations want to protect their technology, governments want their plans kept secret, political dissidents want their identities to be secret, ...

Edward Snowden claims American and British spies hacked into the world’s largest SIM manufacturer

Medical data online

Please send Alice’s record

Please store S_A as Alice’s updated record

Yes, doctor!

How it would work if security was not an issue …

I don’t want the emails or chats I send or receive to be modified or faked. I don’t want my allergy information to be erased from my medical record. I don’t want my accounts to be broken into. I don’t want the data I communicate to my bank to be modified.

Servers don’t want to hacked into. Companies want to control access to their databases.

I want to be sure that entities I interact with are who they claim to be, whether it be my friend Alice, my doctor or google.

Scripps
Security of medical data online

Security concerns

Authenticity and Identity
Was $R_A$ really sent by Scripps?
Even if so, was it modified en route?
Modification could maliciously erase the fact that Alice has a deadly allergy, change medication history, ...

Security of medical data online

Authenticity and Identity
Was $R_A$ really sent by Scripps?
Even if so, was it modified en route?
Is the retrieve request really from Alice's doctor?
Is the store request really from Alice's doctor?
Even if so, was $S_A$ modified en route?

Security concerns

Privacy
Eavesdroppers should not get Alice's record.
Doctor's diagnosis should remain private.
That Alice even saw the doctor is nobody's business but hers.

Security concerns

Glenn Greenwald
If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.

Eric Schmidt, CEO
Google, 2009
If you have nothing to hide then give me the passwords to ALL your email accounts, your text and chat histories, ...

Why privacy matters

Bruce Schneier
The Value of Privacy
Privacy protects us from abuses by those in power … We keep private journals, sing in the shower … privacy is a basic human need.

The Chronicle of Higher Education
Why privacy matters even if you have nothing to hide http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/

You are under surveillance right now.

Your cell phone provider tracks your location and knows who's with you. Your online and in-store purchasing patterns are recorded, and reveal if you're unemployed, sick, or pregnant. Your e-mails and texts expose your intimate and casual friends. Google knows what you are thinking because it saves your private searches. Facebook can determine your sexual orientation without your ever mentioning it.

The powers that surveil us do more than simply store this information. Corporations use surveillance to manipulate not only the news articles and advertisements we each see, but also the prices we're offered. Governments use surveillance to discriminate, censor, chill free speech, and put people in danger worldwide. And both sides share this information with each other or, even worse, lose it to cybercriminals in huge data breaches.

Much of this is voluntary: we cooperate with corporate surveillance because it promises us convenience, and we submit to government surveillance because it promises us protection. The result is a mass surveillance society of our own making. But have we given up more than we have gained?

"The generous explanation for Schmidt's statement is that he's revolutionized his thinking since 2005, when he blacklisted CNET for publishing info about him gleaned from Google searches, including salary, neighborhood, hobbies and political donations. In that case, the married CEO must not mind the coverage of his various reputed girlfriends …" Ryan Tate, 12/04/09.

Academic cryptographers often represent the adversary like this

But ADVERSARIES are REAL

Sony Pictures Entertainment hack

From Wikipedia, the free encyclopedia

The Sony Pictures Entertainment hack was a release of confidential data belonging to Sony Pictures Entertainment on November 24, 2014. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films, and other information. The hackers called themselves the "Guardians of Peace" or "GOP" and demanded the cancellation of the planned release of the film The Interview, a comedy about a plot to assassinate North Korean leader Kim Jong-un. United States intelligence officials, evaluating the software, techniques, and network sources used in the hack, allege that the attack was sponsored by North Korea. North Korea has denied all responsibility, and some cybersecurity experts have cast doubt on the evidence, alternatively proposing that current or former Sony Pictures employees may have been involved in the hack.

WARNING

Well, kind of …

But these are not precise terms or distinctions. One should be wary of debating terms rather than issues!


The economy of cybercrime

Fascinating chain from spam to banks to goods

How Viagra spam works

The Snowden revelations

Court-approved NSA access to Google and Yahoo accounts
Verizon hands phone records of millions of customers to NSA daily
Extensive wiretapping, tapping undersea cables
Harvesting of millions of email and instant-messaging contact lists
Tracking and mapping location of cellphones
Backdoor planted in Dual_EC_DRBG random-number generator
Paying corporations to adopt NSA-broken standards
Sophisticated malware

...
Academic cryptographers often represent the adversary like this.

Instead think of the adversary as a well-funded, technically capable and highly motivated entity with lots of computing power.

Put on your adversary hat!

Ask what are the risks and threats. Ask how the system might be attacked. Be critical of security claims.

Our system is secure because it uses 128-bit AES encryption!

Really? How exactly is AES used? What precisely are the security claims? What is the threat model? Do you have a security proof?

Have as goal for this course to develop the security mindset!

Investigate what is pointed to above: Watch the videos, read the books and news. Have an informed and rational opinion in the privacy debate. It will be on the quiz!

Be aware! Be shocked! Be afraid!

Name some security concerns that you have and classify them as privacy, authenticity or other.

Develop a security mindset! Look for how and why an adversary might break things.

Truth or exaggeration? If true, can we change it?

If it’s on the Internet, it isn’t private.

A HELPFUL VENN DIAGRAM
Secure Channels

A secure channel

Alice

Bob

Privacy: Adversary does not learn anything about $M_A$, $M_B$

Authenticity: $M'_A = M_A$ and $M'_B = M_B$

The ideal channel: A kryptonite pipe

Made of kryptonium

Adversary

Even Superman can’t violate privacy or integrity

But kryptonite is in short supply since the planet Krypton exploded.

Cryptography is used to build a secure channel

Privacy: Adversary does not learn anything about $M_A$, $M_B$

Authenticity: $M'_A = M_A$ and $M'_B = M_B$
But who are "Alice" and "Bob"?

The question of identity

Cryptography is used to build a secure channel

Names are bound to people via societal means

A secure channel

Privacy: Adversary does not learn anything about $M_A$, $M_B$

Authenticity: $M'_A = M_A$ and $M'_B = M_B$

Identity: Alice is really "Alice" and Bob is really "Bob"

But what does that mean?

Cryptography

Adversary

Established out-of-band binding of name to person

But what does that mean?
Identity on the Internet

These are difficult issues

Established how?
What do `domain name` and `entity` even mean?

binding of domain name to entity

Secure channels

Establishing a secure channel is the most basic task of cryptography. We want to do it, and do it right.

But what exactly is a secure channel anyway?

Good question! We need a definition that is precise and useful.

TLS/SSL

Did you use any cryptography today?
Whether you knew it or not, you likely did.

What tasks beyond these should cryptography address?
11,748 Android apps use cryptography. 10,327 of them get it wrong [EBFK13].

Username and password are sent over TLS/SSL.

Credit-card number is sent over TLS/SSL.

TLS/SSL aims to provide a secure channel.

**Privacy:** Adversary does not learn anything about $M_A$, $M_B$

**Authenticity:** $M'_A = M_A$ and $M'_B = M_B$

**Identity:** Alice is really "Alice" and Bob is really "Bob".

The cryptographic core of TLS/SSL

\[ \text{Alice’s AKE module} \quad \text{Bob’s AKE module} \]

\( K \) is a fresh, authentic session key.

Adversary cannot influence or know \( K \).
The question of identity: Who are ``Alice'' and ``Bob''?

On the Internet, nobody knows you are a dog.

Who is ``Bob''?

Think of Bob = example.com as a url or an ip address

Certificate authorities

As of February 2015
But who is "Alice?"

- AliceWonder@wonderland
- AliceWaters@chezpanisse
- AliceWalker@colorpurple
- AlicePoker@saloon

Default TLS/SSL provides unilateral authentication: Bob authenticates himself to Alice but not vice versa.

Alice does not typically have a certificate. Alice will typically authenticate herself to Bob with username and password over the TLS/SSL channel itself.

TLS/SSL Vulnerabilities

POODLE vulnerability hastens the death of SSL 3.0

FREAK Attacks SSL/TLS Security, Putting Apple, Android Users at Risk

Heartbleed: "Secure" internet wasn't safe

Security researchers have uncovered a fatal flaw in a key safety feature for surfing the Web -- the one that keeps your email, banking, shopping, passwords and communications private.
Many different TLS/SSL Implementations:
OpenSSL, GnuTLS, cryptlib, JSSE, RSA BSafe, SChannel, ...

Issues: Cipher suites, re-negotiation, side-channels, buffer overflows, bad randomness, ...

Lots of bad crypto in TLS/SSL, often for historic and legacy reasons.

Summary, take away

TLS/SSL: Appreciate that there is a ton going on every time you access a website!

Providing a well-designed and analyzed cryptographic core is a central problem for us to address.
Cryptographic schemes

\( E \): encryption algorithm
\( D \): decryption algorithm
\( K_e \): encryption key
\( K_d \): decryption key

Settings:
- public-key (asymmetric): \( K_e \) public, \( K_d \) secret
- private-key (symmetric): \( K_e = K_d \) secret

Algorithms: standardized, implemented, public!

How do keys get distributed? Magic, for now!
Cryptographic schemes

Our concerns:
• How to define security goals?
• How to design $E$, $D$?
• How to gain confidence that $E$, $D$ achieve our goals?

Early history

Substitution ciphers/Caesar ciphers:

$K_e = K_d = \pi: \Sigma \rightarrow \Sigma$, a secret permutation

e.g., $\Sigma = \{A, B, C, \ldots\}$ and $\pi$ is as follows:

\[
\begin{array}{c|c|c|c|c|c|c|c}
\sigma & A & B & C & D & \cdots \\
\hline
\pi(\sigma) & E & A & Z & U & \cdots \\
\end{array}
\]

$E_{\pi}(CAB) = \pi(C)\pi(A)\pi(B) = Z \ E \ A$

$D_{\pi}(ZEA) = \pi^{-1}(Z)\pi^{-1}(E)\pi^{-1}(A) = C \ A \ B$

Not very secure! (Common newspaper puzzle)

Why is cryptography hard?

• One cannot anticipate an adversary strategy in advance; number of possibilities is infinite.
• “Testing” is not possible in this setting.
The age of machines

**Enigma:** German World War II machine

Broken by British in an effort led by Turing

---

**Shannon and One-Time-Pad (OTP) Encryption**

\[ K_e = K_d = K \xleftarrow{\text{random}} \{0,1\}^k \]

For any \( M \in \{0,1\}^k \)
\[ - E_K(M) = K \oplus M \]
\[ - D_K(C) = K \oplus C \]

Theorem (Shannon): OTP is perfectly secure as long as only one message encrypted.

“Perfect” secrecy, a notion Shannon defines, captures mathematical impossibility of breaking an encryption scheme.

Fact: if \( |M| > |K| \), then no scheme is perfectly secure.

---

**Modern Cryptography: A Computational Science**

Security of a “practical” system must rely not on the impossibility but on the computational difficulty of breaking the system.

(“Practical” = more message bits than key bits)
Rather than:

“It is impossible to break the scheme”

We might be able to say:

‘No attack using \( \leq 2^{160} \) time succeeds with probability \( \geq 2^{-20} \)”

I.e., Attacks can exist as long as cost to mount them is prohibitive, where Cost = computing time/mem, $$$

Defining security

Being able to precisely (formally, mathematically) state what is the security goal of a design is challenging but important.

We will spend a lot of time developing and justifying strong, precise notions of security.

Thinking in terms of these precise goals and understanding the need for them may be the most important thing you get from this course!

Defining Security

What does it mean for an encryption scheme to provide privacy?

Does it mean that given \( C = E_{K_a}(M) \), adversary cannot

- recover \( M \)?
- recover the first bit of \( M \)?
- recover the XOR of the first and the last bits of \( M \)?
- ...

We will provide a formal definition for privacy, justify it, and show it implies the above (and more).
### Lego Approach

We typically design high-level primitives from atomic ones.

```
Atomic primitive
↑
Transformer
↑
High-level primitive
```

### Atomic Primitives or Problems

**Examples:**
- Factoring: Given large $N = pq$, find $p, q$
- Block ciphers: DES, AES, ...
- Hash functions: MD5, SHA1, SHA3, ...

**Features:**
- Few such primitives
- Confidence by cryptanalysis.

**Drawback:** Don’t directly solve any security problem.

### Higher Level Primitives

**Goal:** Solve security problem of direct interest.

**Examples:** encryption, authentication, digital signatures, session-key distribution, ...

### Provable security

Enables us to get transformers for which we can guarantee

```
Atomic primitive secure $\implies$ High-level primitive secure
```

**Proven-secure** schemes in use (TLS, SSH, IPSec, ...):
- HMAC
- OAEP
- ECIES
- ...

This is a theory course! Largely definitions and proofs, although of applied value.

Needed: algorithms, theory of computation, probability theory, a little calculus, and

**Mathematical Maturity**

---

**Math Test**

Don’t get it? Either your **pre-reqs** or your **sense of humor** need work.

---

**Assessments and grades**

- Homeworks
- For MS students: Final Exam that functions as the (mandatory) Comprehensive Exam for course.

Grade based on above and a discretionary score. See course information sheet for details.

I would like to get name-to-face matches for all students!
Rules and policies

• Collaboration with **upto one other CSE207 student** allowed if so indicated on problem set, but each student must **write their own solutions** in their own words.

• Looking at solutions from **previous years** of the course or finding them on the **Internet** is not allowed.

• Non-compliance with rules is reported to UCSD Academic Integrity Office and can result in dismissal.

• Grader expects **neat, mathematically precise** and **well-written solutions**. **Quality of exposition** will impact score.

• Doesn’t work to come back and say “**You did not understand what I meant.**” You have to write in proper mathematical language so that your meaning is clear. You are graded on what you write, not on what you think is in your head.

Administrative

• **READ** course information sheet

• Then **READ**, sign and return affirmation

Resources:

• Lecture **slides**: The ONLY source of materiel

• **Homework solutions**

• No textbook

All resources on course web page. Some handed out.
The DIVORCE: Flipping a coin over the Internet

Thinks he's unsupportive. (Sponges are like that.)

Thinks she's unstable. (She keeps changing size.)

Divorce!

But who gets custody of the Tesla Model S?

HEADS (1):
Alice gets the Tesla

TAILS (0):
Bob gets the Tesla

HEADS (1):
Alice is in Wonderland

TAILS (0):
Bob is underwater

Alice is in Wonderland
Bob is underwater

I'll flip a coin and send you the outcome.

I don't think so.

Alice has the security mindset!

Alice gets herself some hardware ...

Put this $a$ inside and then lock the safe

Locked safe containing $a$

Combination safe

Alice knows the secret combination / key $92093$.

Locked safe containing $a$

Unlock and remove contents

Alice also gets herself some notation ...

Example

$s \leftarrow \$ \{0, 1\}$

$Pr[a = 0] = Pr[a = 1] = \frac{1}{2}$

this is selected at random from this set

symbolizes coins
1. Alice picks a at random and sends Bob a locked safe containing a.

3. Alice sends Bob the key to open the safe.

Output: Alice sets c as shown.

**Claim:** This works, meaning neither party controls the common coin.

**Scenario A:** Bad Alice, Good Bob

Alice is an adversary trying to make Bob output c = 1. Bob follows the protocol.

**Claim A:** Adversary Alice will fail.

**Scenario B:** Bad Bob, Good Alice

Bob is an adversary trying to make Alice output c = 0. Alice follows the protocol.

**Claim B:** Adversary Bob will fail.

---

1. Adversary picks a in any way it wants and sends Bob a locked safe containing a.

3. Adversary sends Bob a key to open the safe.

**Adversary wants to make c = 1.**

So it must set $a = b \oplus 1$

But it can't set $a = b \oplus 1$ because it doesn't know b at the time it picks a.

But this is not enough to establish **Claim A** because Adversary could pick the safe in a devious way ...

---

**Scenario A**

Alice picks a at random and sends Bob a locked safe containing a.

2. Bob picks a bit b at random and sends it to Alice. He keeps the locked safe.

Output: Bob opens the safe using the key to get a and then sets c as shown.

3. Alice sends Bob the key to open the safe.

Output: Alice sets c as shown.

---

**Scenario B**

Bob picks a bit b at random and sends it to Alice. He keeps the locked safe.

Output: Bob opens the safe using the key to get a and then sets c as shown.

---

**Sneaky safes?**

Suppose Adversary Alice could fabricate a sneaky safe and two different keys such that

<table>
<thead>
<tr>
<th>key</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>0</td>
</tr>
</tbody>
</table>

The safe looks normal to me!

1. Adversary fabricates the safe and keys as above and sends the safe to Bob.

2. Bob picks a bit b at random and sends it to Alice. He keeps the locked safe.

Output: Bob opens the safe using the key to get a and then sets c as shown.

This results in $c = 1$, so **Adversary wins.**
Any safe commits its creator to one value for its content.

Sneaky safes? Suppose Adversary Alice could fabricate a sneaky safe and two different keys key₁ and key₂ such that key₁ → 1 and key₂ → 0.

Not possible!

Safes are BINDING: One cannot create key₁ and key₀ such that

Security of the coin-flipping-with-safes protocol relies on the following two facts / assumptions:

Safes are HIDING: Given α, the adversary has no idea what is α. Such that

This is the property we know and understand safes as having.

This is a property safes seem to have but we don’t usually recognize or enunciate.

It is important to formulate and state the assumptions underlying any claim of security.

Coin flipping without hardware: From safes to bits

Sending a safe from Wonderland to Undersea over the Internet is hard.

Can we get a protocol that we can implement fully in software and that only transmits bits?

YES: Via commitment schemes, which we will later formalize and construct.

If Bob can drive a Tesla underwater, why do we bother about a little thing like sending safes over the Internet?

Can you think of other problems one can solve with similar methods?
Can you implement a secure Internet Casino?