



Cryptology

Sabyasachi Karati

Assistant Professor
Cryptology and Security Research Unit (C.S.R.U)
R. C. Bose Centre for Cryptology and Security
Indian Statistical Institute (ISI)
Kolkata, India





Contact

email : skarati.isi@gmail.com,
skarati@isical.ac.in.

Office: : Room 404, 3rd Floor, Deshmukh Building
Indian Statistical Institute
203 Barrackpore Trunk Road
Kolkata 700 108, WB, India.

Office Hours : By Appointment only.



Syllabus

1. Introduction To Cryptography
2. History and Classical Ciphers
3. Basics of Probability Theory
4. Shanon Theory
5. Pseudo-Random Generator and Stream Cipher
6. Cryptoanalysis of Stream cipher
7. Pseudo-Random Permutation and Block cipher
8. Cryptoanalysis of Block cipher
9. Pseudo-Random Function
10. Notion of CPA and CCA
11. Symmetric key Authentication
12. Authenticated Encryption (if time permits)
13. Basics of Number Theory, and Factoring and Computing Discrete Log
14. Private-Key Management and the Public-Key Revolution
15. Diffie-Hellman Key Exchange
16. Public-Key Encryption Schemes
17. CCA Security of PK Encryption
18. Digital Signatures.



Source of Study Materials

Books

- **A Graduate Course in Applied Cryptography** by Dan Boneh and Victor Shoup.
- **Introduction to Modern Cryptography** by Jonathan Katz and Yehuda Lindell.
- **Cryptography - Theory And Practice** by Douglas Stinson.
- **Understanding Cryptography** by Christof Paar.



Source of Study Materials

Books

- **A Graduate Course in Applied Cryptography** by Dan Boneh and Victor Shoup.
- **Introduction to Modern Cryptography** by Jonathan Katz and Yehuda Lindell.
- **Cryptography - Theory And Practice** by Douglas Stinson.
- **Understanding Cryptography** by Christof Paar.

Lecture Series

You can also follow the lecture series by Dan Boneh and Mihir Bellare.



Lecture 01

Introduction To Cryptology



Cryptology



Wikipedia

- The word [cryptography](#) comes from Greek words: [kryptós-graphein](#).
- The word [cryptology](#) comes from Greek words: [kryptós-logia](#).



Wikipedia

- The word [cryptography](#) comes from Greek words: [kryptós-graphein](#).
- The word [*cryptology*](#) comes from Greek words: [kryptós-logia](#).
 - [kryptós](#) means [hidden, secret](#).
 - [graphein](#) means [to write](#).
 - [logia](#) means [study](#).



Cryptology

Wikipedia

- The word [cryptography](#) comes from Greek words: [kryptós-graphein](#).
- The word [cryptology](#) comes from Greek words: [kryptós-logia](#).
 - [kryptós](#) means [hidden, secret](#).
 - [graphein](#) means [to write](#).
 - [logia](#) means [study](#).

Oxford Dictionary

[The study of codes, or the art of writing and solving them.](#)



Cryptology: Is it art or science?



Cryptology: Is it art or science?

Was Art

- Was indeed the case till late 20th century.
- Till then constructing good codes, or breaking existing ones, relied on **creativity** and a **developed sense** of how codes work.
- There was **little theory** to rely on.
- For a long time, there was **no working definition** of what constitutes a good code.



Cryptology: Is it art or science?

Was Art

- Was indeed the case till late 20th century.
- Till then constructing good codes, or breaking existing ones, relied on **creativity** and a **developed sense** of how codes work.
- There was **little theory** to rely on.
- For a long time, there was **no working definition** of what constitutes a good code.



Figure: “Cryptex” from the movie “The Da Vinci Code”.



Cryptology: Is it art or science?

Is Science Now

- 1970's and 1980's: This picture of cryptography radically changed.
- A rich theory began to emerge, enabling the rigorous study of cryptography as a *science* and a *mathematical discipline*.
- This perspective has, in turn, influenced how researchers think about the broader field of *computer security*.

Is Alive

- Cryptography is still *evolving*.
- Researchers are continuing to construct and *change* it depending on the *change of the security notion*.



Adversary

Adversary

- In cryptography, there exists a **special entity**, called **Adversary**
 - Adversary tried to subvert what we are doing,
 - Tries to use our actions towards their advantage.
- A major part of cryptography deals with:
 - Understanding the **intention** and the **behavior** of the adversary,
 - **Formalizing** and **modeling** them,
 - Developing algorithms to **overcome the effect of the Adversary**.



Adversaries are Everywhere

Print subscriptions Sign in Search jobs Search International edition -

Support the Guardian

Available for everyone, funded by readers

Support us →

News Opinion Sport Culture Lifestyle More ▾

World UK Coronavirus Climate crisis Environment Science Global development Football Tech Business Obituaries

Meta

This article is more than 1 month old

Facebook sued for collecting personal data to target adverts

In high court case that could set precedent for millions, Tanya O'Carroll alleges owner Meta is breaking UK data laws

Don Milmo Global technology editor

Mon 21 Nov 2022 14.53 GMT

A photograph showing a person's hand holding a smartphone. The screen displays the Facebook logo and interface.

USA TODAY

For You News Sports Entertainment Life Money Tech Travel Opinion GET YOUR TICKETS

Advertisement

How Facebook can have your data even if you're not on Facebook

Edward C. Baig USA TODAY

Published 4:57 p.m. ET April 13, 2018 | Updated 8:31 a.m. ET April 16, 2018

Facebook Add Topic

The point one nat can't be covered from just two co USA TODA



Adversaries are Everywhere

INDIA TODAY DAVID INDIATODAY MAHALALAM BUSINESS TODAY AADTAI LALLANTOP BANGLA GATV KOLKATA

INDIA TODAY

Dark Mode Premium

Home Personalise Live TV India World Business Technology Showbuzz Sports Science Health News Analysis Magazine Trending NewsMo

Google collects most amount of user data and this app alerts every time your data is tracked

Google has been found to be collecting the highest amount of user data among all the other tech companies, including Facebook, Amazon, Apple and others.

ADVERTISEMENT

Creditline: From the Industry Leader

Ankita Chatterjee New Delhi, UPDATED: Aug 26, 2022 15:19 IST

HT TECH MAKE LIFE EASIER

Search for news, reviews, lifestyle, technology etc...

HOME NEWS MOBILE LAPTOPS/PC HOW TO GADGETS RECOMMENDER COMPARE PHOTOS VIDEOS WEBSITE

Home > Tech > News > Google is reportedly collecting data from rival apps to improve its own products

Google is reportedly collecting data from rival apps to improve its own products

Google has been collecting and studying usage data from competing apps to help develop its own apps better.

By HT TECH | Updated on: Aug 20 2022, 22:13 IST

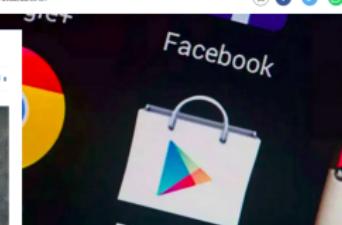
Google fined \$60 million over Android location data collection

By Sergio Gutierrez | August 18, 2022, 11:08 AM

The Australian Competition and Consumer Commission (ACCC) announced that Google was fined \$90 million for misleading Australian Android users regarding the collection and use of their location data for about two years, between January 2017 and December 2018.

The Australian competition watchdog said the tech giant continued tracking some of its users' Android phones even though they had disabled "Location History" in the device's settings.

While customers were misled into thinking that setting would disable location tracking, another account setting turned on by default and named "Web & App Activity" enabled the company "to collect, store and use personally identifiable location data."





Adversaries are Everywhere



Figure: The Snowden Revelations

[https://www.businessinsider.in/this-is-everything-edward-snowden-revealed-in-one-year-of-unprecedented-top-secret-leaks/articleshow/54367926 .cms](https://www.businessinsider.in/this-is-everything-edward-snowden-revealed-in-one-year-of-unprecedented-top-secret-leaks/articleshow/54367926.cms)

- With a top-secret court order, the NSA collected the telephone records from millions of Verizon customers.
- The NSA has the ability to access user data for most major smartphones on the market, including Apple iPhones, Blackberries, and Google Android phones
- The NSA collected more than 250 million email contact lists from services such as Yahoo and Gmail.
- The NSA has the ability to decrypt the common A5/1 cellphone encryption cipher
- The NSA secretly paid computer security firm RSA \$10 million to implement a "back door" into its encryption.
- The NSA physically intercepts routers, servers, and other computer networking equipment before it's exported outside the US, implants "back door" surveillance tools, then repackages them with a factory seal and ships them out, and so on.



Security Goals

- Privacy or Confidentiality,
- Authenticity,
- Identity, and so on.



Security Goals

Privacy

Privacy is the ability of an individual or group to keep information or data hidden from all but the authorized ones.



Security Goals

Privacy

Privacy is the ability of an individual or group to keep information or data hidden from all but the authorized ones.

- I do not want others to know **my emails, chats, my ATM Pin, Online banking passwords** and so on.



Security Goals

Privacy

Privacy is the ability of an individual or group to keep information or data hidden from all but the authorized ones.

- I do not want others to know **my emails, chats, my ATM Pin, Online banking passwords** and so on.
- Big companies like to keep their **products formula** secret.



Security Goals

Privacy

Privacy is the ability of an individual or group to keep information or data hidden from all but the authorized ones.

- I do not want others to know my emails, chats, my ATM Pin, Online banking passwords and so on.
- Big companies like to keep their products formula secret.
- Government may want to keep their future action or plan or policies secret.



Security Goals

Privacy

Privacy is the ability of an individual or group to keep information or data hidden from all but the authorized ones.

- I do not want others to know **my emails, chats, my ATM Pin, Online banking passwords** and so on.
- Big companies like to keep their **products formula** secret.
- Government may want to keep their **future action or plan or policies** secret.
- Military may want to keep their **communications** secret.



Security Goals

Authenticity

Data Authenticity implies that the data has not been altered by unauthorized means. On the other hand, Entity Authenticity implies that the data we receive is from the entity from whom it should be.



Security Goals

Authenticity

Data Authenticity implies that the data has not been altered by unauthorized means. On the other hand, Entity Authenticity implies that the data we receive is from the entity from whom it should be. Also known as **Data Integrity**.



Security Goals

Authenticity

Data Authenticity implies that the data has not been altered by unauthorized means. On the other hand, Entity Authenticity implies that the data we receive is from the entity from whom it should be. Also known as **Data Integrity**.

- I do not want **emails or chat** I sent to be modified or faked.



Security Goals

Authenticity

Data Authenticity implies that the data has not been altered by unauthorized means. On the other hand, Entity Authenticity implies that the data we receive is from the entity from whom it should be. Also known as **Data Integrity**.

- I do not want **emails or chat** I sent to be modified or faked.
- I do not want my **communication with my bank server** gets modified.



Security Goals

Authenticity

Data Authenticity implies that the data has not been altered by unauthorized means. On the other hand, Entity Authenticity implies that the data we receive is from the entity from whom it should be. Also known as **Data Integrity**.

- I do not want **emails or chat** I sent to be modified or faked.
- I do not want my **communication with my bank server** gets modified.
- I do not want my **medical data** to be altered or the doctor who is treating me does not want to have **modified medical data** of me. Otherwise, my treatment will be wrong.



Security Goals

Authenticity

Data Authenticity implies that the data has not been altered by unauthorized means. On the other hand, Entity Authenticity implies that the data we receive is from the entity from whom it should be. Also known as **Data Integrity**.

- I do not want **emails or chat** I sent to be modified or faked.
- I do not want my **communication with my bank server** gets modified.
- I do not want my **medical data** to be altered or the doctor who is treating me does not want to have **modified medical data** of me. Otherwise, my treatment will be wrong.
- Companies do not want their **servers to be hacked** and **stored data to be altered**.



Security Goals

Identity

We should be able to be sure that the entities we interact with are who they claim to be.



Security Goals

Identity

We should be able to be sure that the entities we interact with are who they claim to be. Also known as [Source Authentication](#).



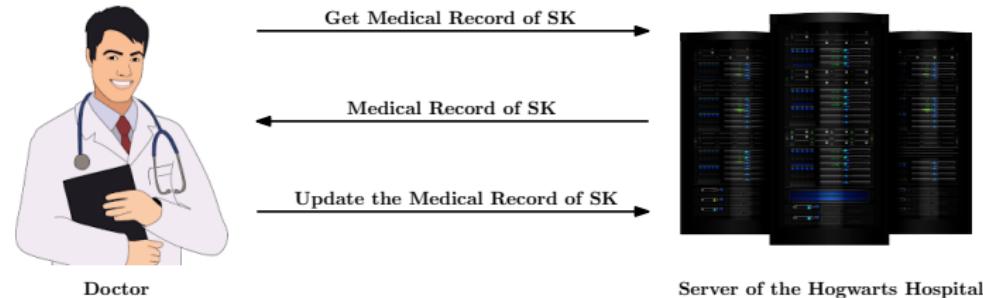
Security Goals

Identity

We should be able to be sure that the entities we interact with are who they claim to be. Also known as [Source Authentication](#).

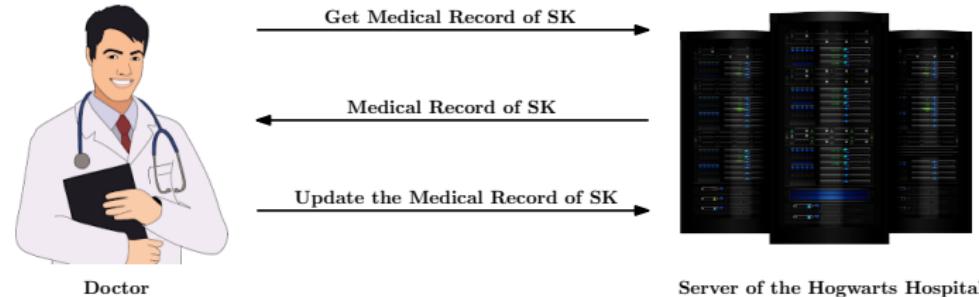


Security Goals Through Example





Security Goals Through Example



Ideal Scenario

- No Adversary,
- No Security Concern.



Security Goals Through Example





Security Goals Through Example

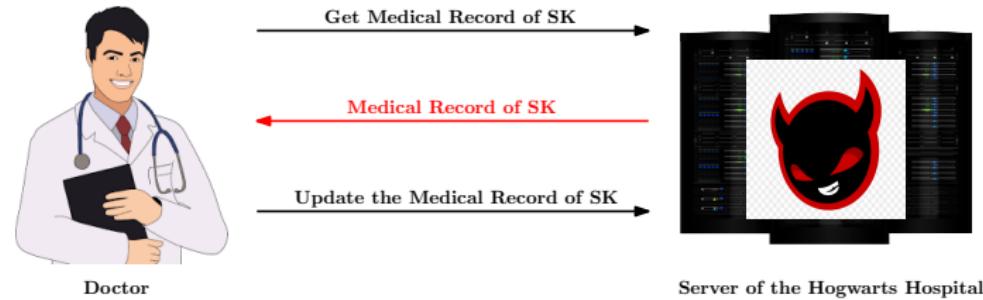


Privacy

- No one must learn about my medical condition.

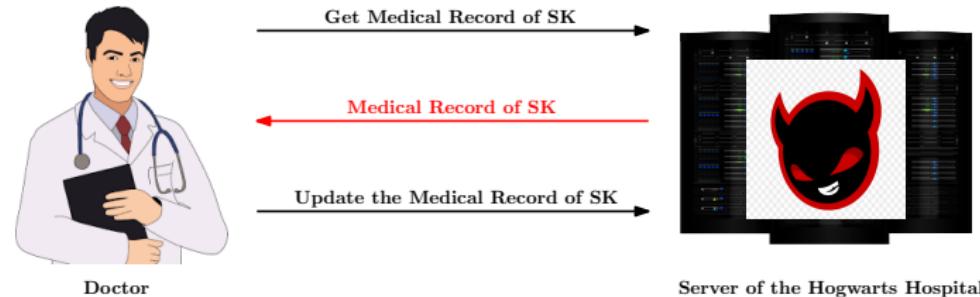


Security Goals Through Example





Security Goals Through Example

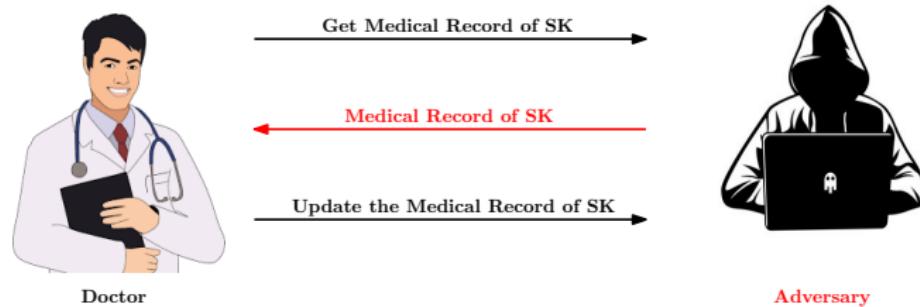


Data Integrity

- My medical condition must not get altered in the hospital server.

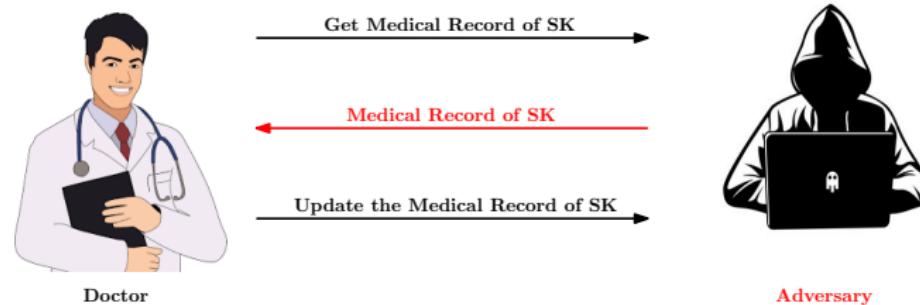


Security Goals Through Example





Security Goals Through Example



Authentication

- Doctor must be able to confirm that the received medical report is indeed from the hospital server.



Why is Privacy Important?



About Issues Our Work Take Action Tools [Donate](#) Q

Google CEO Eric Schmidt Dismisses the Importance of Privacy

NEWS UPDATE BY RICHARD ESGUERRA | DECEMBER 10, 2009

Yesterday, the web was buzzing with commentary about Google CEO Eric Schmidt's dangerous, dismissive response to concerns about search engine users' privacy. When [asked](#) during an interview for CNBC's recent "Inside the Mind of Google" special about whether users should be sharing information with Google as if it were a "trusted friend," Schmidt responded, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."



nts in your



Why is Privacy Important?

Mark Zuckerberg buys up all the properties around his house so he can live in his own neighbourhood

by Alessandro Renesis | Last updated on May 26, 2022 at 3:22PM | Published on Mar 21, 2022 | LIFESTYLE, MANSIONS





Why is Privacy Important?

Glenn Greenwald can't get anyone to take this challenge

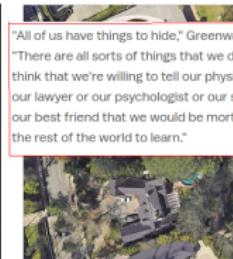
By German Lopez | @germanlopez | german.lopez@voxy.com | Oct 13, 2014, 9:50am EDT



SHARE

Greenwald has devised a challenge for people that tell him they don't worry about their privacy because they have nothing to hide: He asks them to send him all their email passwords and allow him to look through and publish anything he finds interesting. "After all, if you're not a bad person, if you're doing nothing wrong, you should have nothing to hide," Greenwald quipped. "Not a single person has taken me up on that offer."

The video thumbnail shows Glenn Greenwald speaking on stage at a TED event. He is wearing a blue shirt and gesturing with his hands. The background is dark with stage lights. A YouTube play button icon is overlaid on the video frame. At the bottom left, there is a 'Watch on YouTube' button.

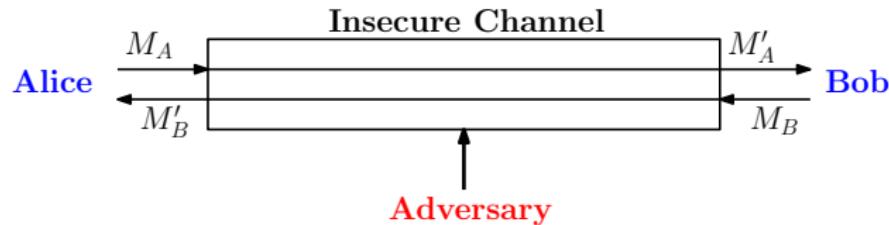




Cryptography

Definition

Cryptography is a means to enable parties to maintain privacy of the information they send to each other, even in the presence of an adversary with access to the communication channel.

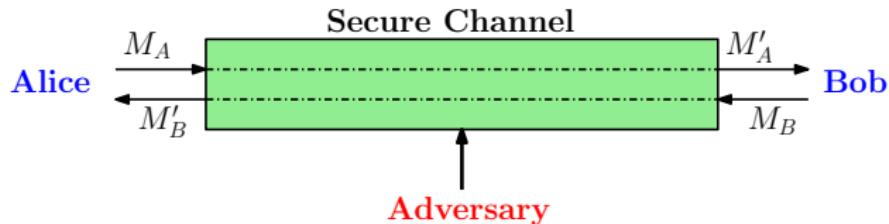




Cryptography

Definition

Cryptography is a means to enable parties to maintain privacy of the information they send to each other, even in the presence of an adversary with access to the communication channel.

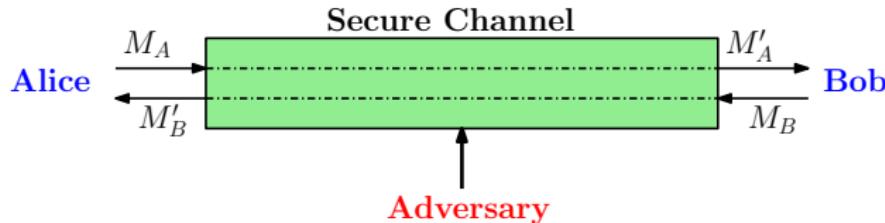




Cryptography

Definition

Cryptography is a means to enable parties to maintain privacy of the information they send to each other, even in the presence of an adversary with access to the communication channel.



Secure Channel

Main objective of Cryptography is the **Creation of a Secure Channel**. Establishing secure channel means to achieve:

- **Privacy:** Adversary does not learn anything about M_A and M_B .
- **Authenticity:** $M_A = M'_A$ and $M_B = M'_B$.
- **Identity:** Alice is really “Alice” and Bob is really “Bob”.



Consumers of Cryptography

Earlier (before 1980's)

Military organizations and governments.



Consumers of Cryptography

Earlier (before 1980's)

Military organizations and governments.

Now (after 1980's)

Cryptography is **everywhere!** It is used

- while authenticating oneself by typing a password,
- while purchasing items by credit card over the Internet,
- while downloading a verified update for your operating system.



Consumers of Cryptography

Earlier (before 1980's)

Military organizations and governments.

Now (after 1980's)

Cryptography is **everywhere!** It is used

- while authenticating oneself by typing a password,
- while purchasing items by credit card over the Internet,
- while downloading a verified update for your operating system.

Summary

- It has changed from a **heuristic** set of tools concerned with ensuring secret communication for the **military** to a **science** that helps secure systems for **ordinary people** all across the globe.
- Meaning that it has become a more central topic within CS.



Where do we use of Cryptography

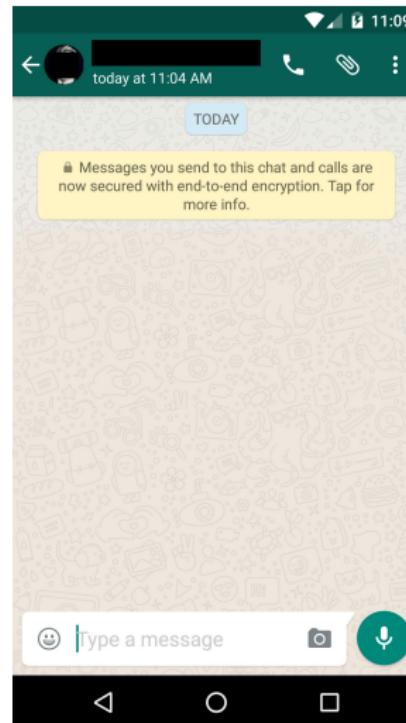


Figure: Whatsapp



Where do we use of Cryptography

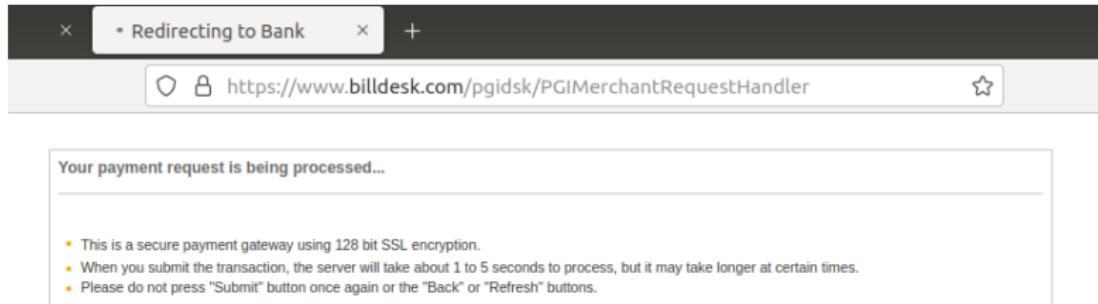


Figure: Billdesk Online Transaction



Where do we use of Cryptography

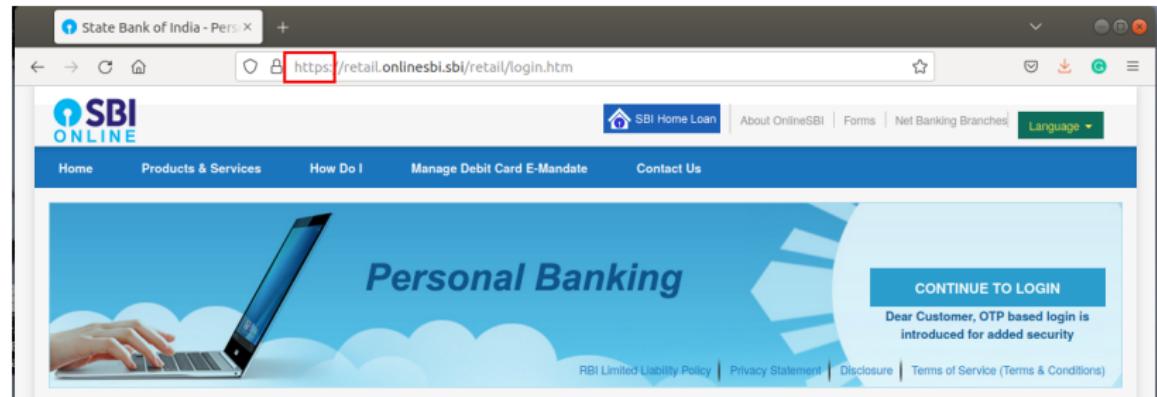


Figure: Transport Layer Security (TLS)



Where do we use of Cryptography

State Bank of India - Pers X

https://retail.onlinesbi.sbi/retail/login.htm

SBI ONLINE

Page Info — https://retail.onlinesbi.sbi/retail/login.htm

General Media Permissions Security

Website Identity

Website: retail.onlinesbi.sbi
Owner: STATE BANK OF INDIA
Verified by: DigiCert Inc

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? Yes, cookies and 66 bytes of site data

Have I saved any passwords for this website? No

Technical Details

Connection Encrypted [TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2]

The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

CONTINUE TO LOGIN

Dear Customer, OTP based login is introduced for added security

Terms of Service (Terms & Conditions)

ALWAYS

keep your computer free of malware

NEVER

reveal your passwords or card details to anyone

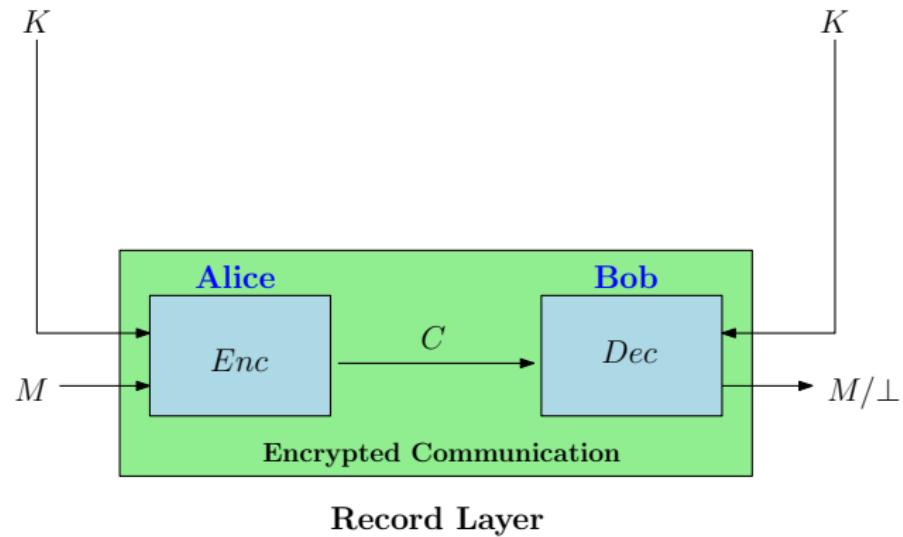
Please ensure the following before log

- The URL in your browser address bar begins with "https".
- The address or status bar displays the lock icon.
- Phishing is a fraudulent attempt, usually made through email, phone calls, SMS etc seeking your personal and confidential information.

Figure: Transport Layer Security (TLS)

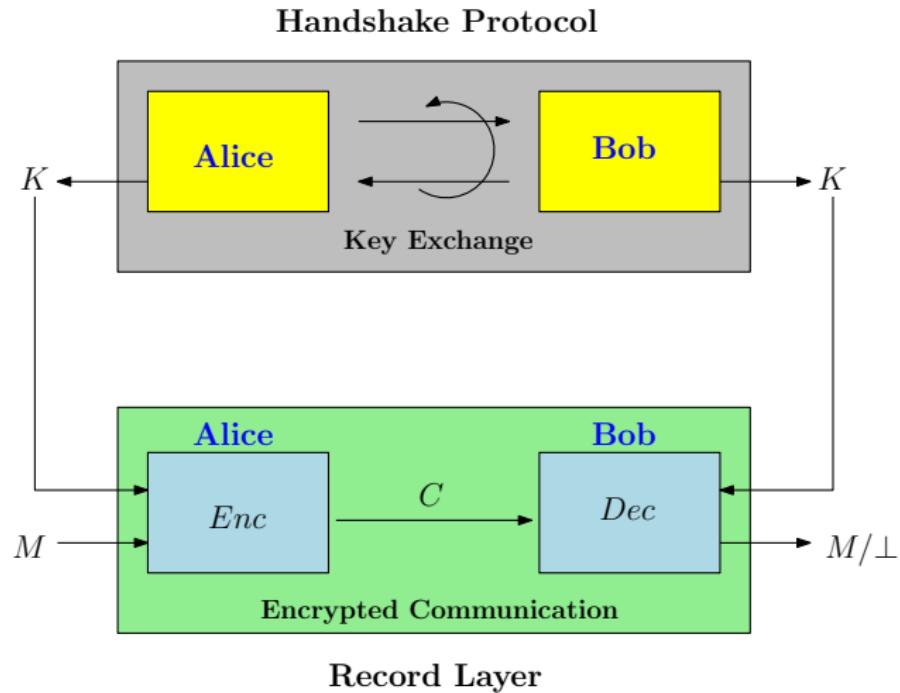


Basic of TLS/SSL



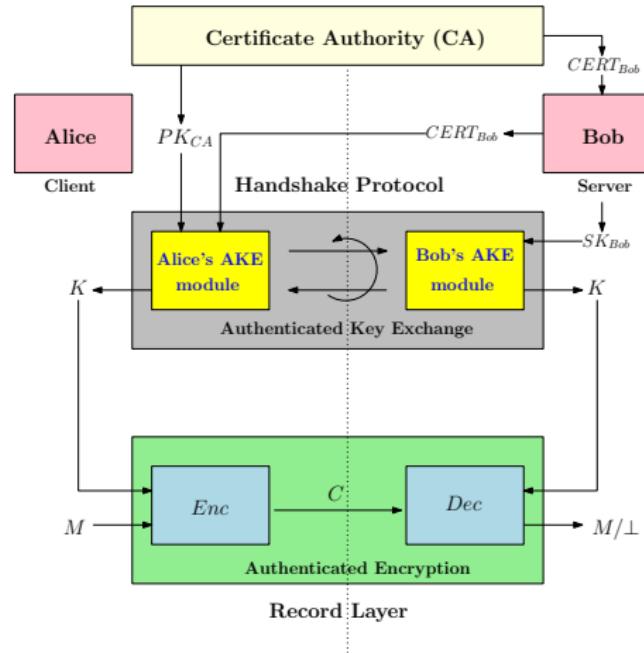


Basic of TLS/SSL



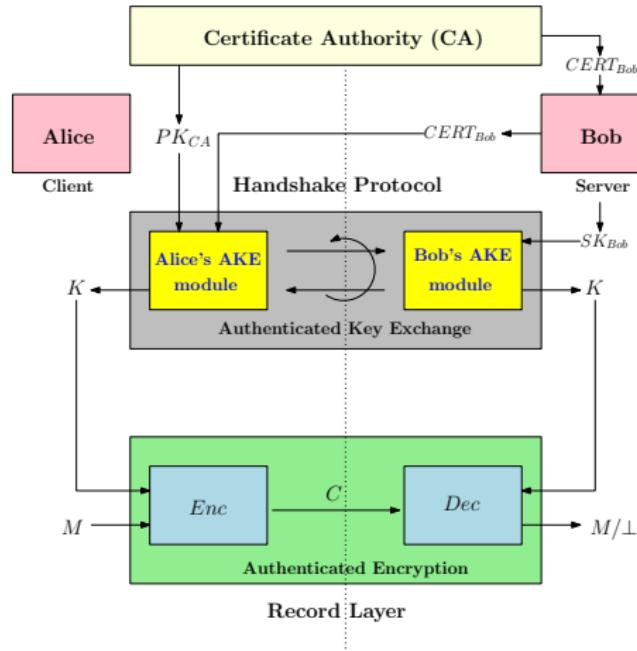


A more detailed view of TLS/SSL





A more detailed view of TLS/SSL



- By default, TLS/SSL provides **unilateral authenticating**, that is Bob authenticate himself.
- Alice does not have any certificate normally.
- Alice typically authenticate herself using **username and password** over the TLS/SSL channel created.



Vulnerabilities of TLS/SSL

Vulnerability	Crypto	Implementation/ Usage
FREAK	x	
Re-negotiation	x	
Version Rollback		x
BEAST	x	
Padding Oracle	x	
Lucky 13	x	
Poodle	x	x
Heartbleed		x
RC4	x	
AllYourSSLSAreBelongToUs		x



Vulnerabilities of TLS/SSL

Vulnerability	Crypto	Implementation/ Usage
FREAK	x	
Re-negotiation	x	
Version Rollback		x
BEAST	x	
Padding Oracle	x	
Lucky 13	x	
Poodle	x	x
Heartbleed		x
RC4	x	
AllYourSSLSAreBelongToUs		x

- Many different implementations of TLS/SSL: OpenSSL, GnuTLS, cryptlib, RSA, SChannel and so on.
- Issues: Cipher suits (Crypto), re-negotiation (Denial of Service), side channel, buffer overflow(Implementation), bad randomness (Crypto/Implementation), and so on.
- Lots of **bad crypto** in TLS/SSL, often for historic and legacy reasons.



Vulnerabilities of TLS/SSL

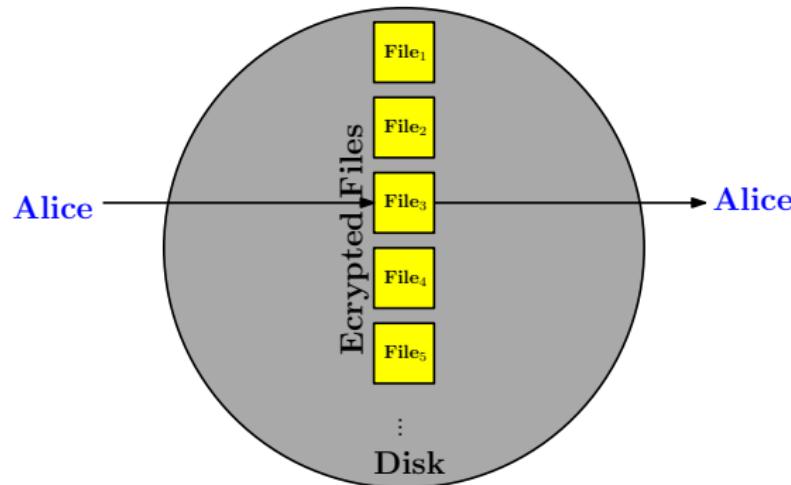
Vulnerability	Crypto	Implementation/ Usage
FREAK	x	
Re-negotiation	x	
Version Rollback		x
BEAST	x	
Padding Oracle	x	
Lucky 13	x	
Poodle	x	x
Heartbleed		x
RC4	x	
AllYourSSLSAreBelongToUs		x

- Many different implementations of TLS/SSL: OpenSSL, GnuTLS, cryptlib, RSA, SChannel and so on.
- Issues: Cipher suits (Crypto), re-negotiation (Denial of Service), side channel, buffer overflow(Implementation), bad randomness (Crypto/Implementation), and so on.
- Lots of **bad crypto** in TLS/SSL, often for historic and legacy reasons.

Do Crypto and Get it right.



Other Applications of Cryptography



Encrypting Files on Disk

- Algorithms: Encrypting File System (EFS), TrueCrypt.
- Analogs to secure communication: Alice today sends a message to Alice in Future.



Other Applications of Cryptography

- Digital Signatures,
- eVoting System,
- Private Auction,
- Privately outsourcing computation,
- Zero Knowledge, and many more.



Keep in Mind

Cryptography is

- A fabulous and cool tool.
- core of many security mechanisms.



Keep in Mind

Cryptography is

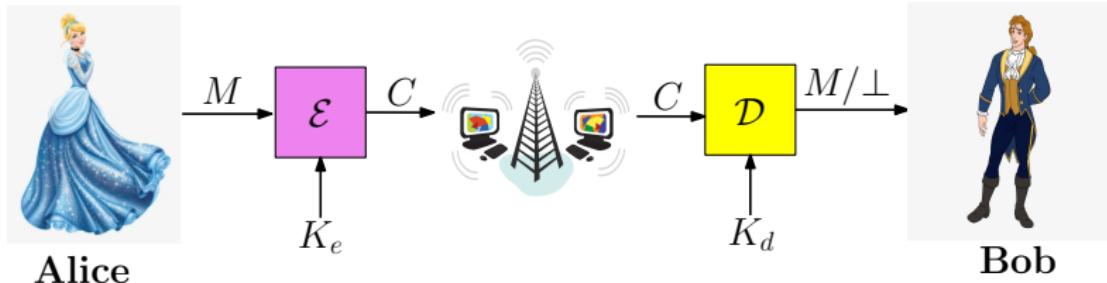
- A fabulous and cool tool.
- core of many security mechanisms.

Cryptography is not

- Solution to every security problems.
- Reliable unless implemented and used properly.
- Something you should try to invent yourself: many many examples of broken ad-hoc designs.



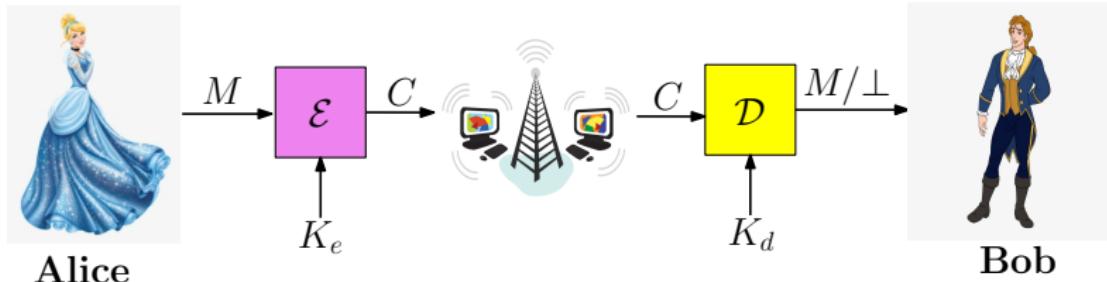
Cryptographic Schemes



- \mathcal{E} : Encryption algorithm, and K_e : Encryption key.
- \mathcal{D} : Decryption algorithm, and K_d : Decryption key.
- M : Plain text or Message, and C : Cipher text or Encrypted message.



Cryptographic Schemes



- \mathcal{E} : Encryption algorithm, and K_e : Encryption key.
- \mathcal{D} : Decryption algorithm, and K_d : Decryption key.
- M : Plain text or Message, and C : Cipher text or Encrypted message.

Settings

- Symmetric Key: $K_e = K_d$. (First half of this course) and We will assume that keys are obtained Magically
- Asymmetric Key or Public Key: $K_e \neq K_d$. (Second half of this course).



End