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

Cryptology

Wikipedia

- The word cryptography comes from Greek words: kryptós-graphein.
- The word ***cryptology*** comes from Greek words: kryptós-logia.

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.

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 20^{th} 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 20^{th} 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

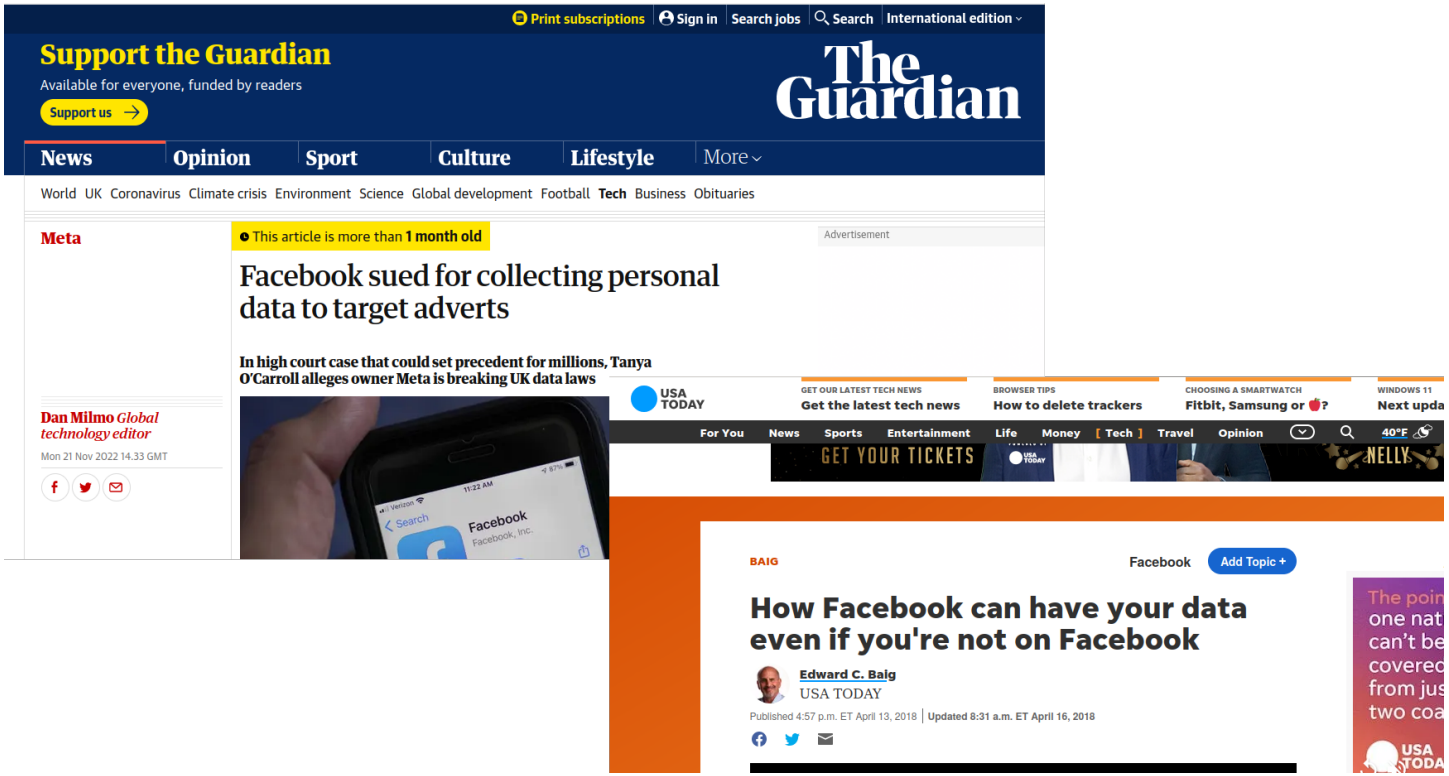
- Cryptography is still evolving.
- Researcher are continuing to construct and change it depending on the change of the security notion.

Adversary

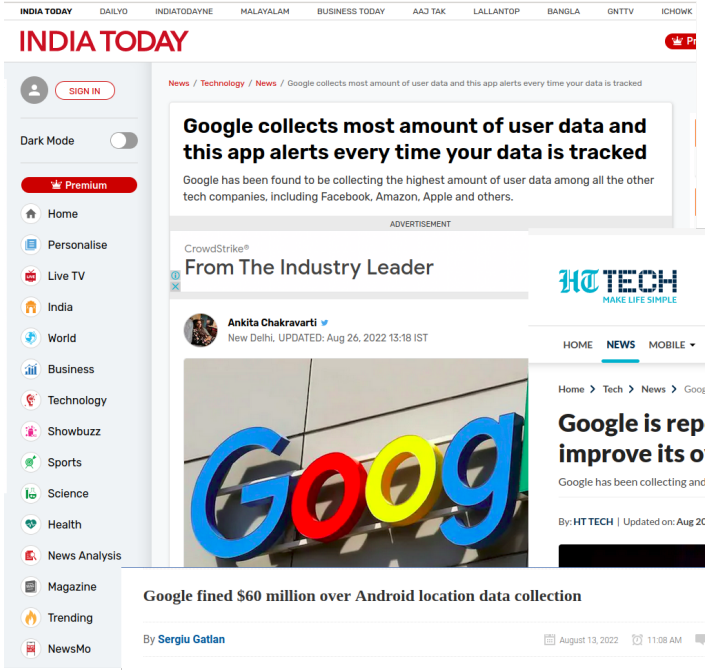
Adversary

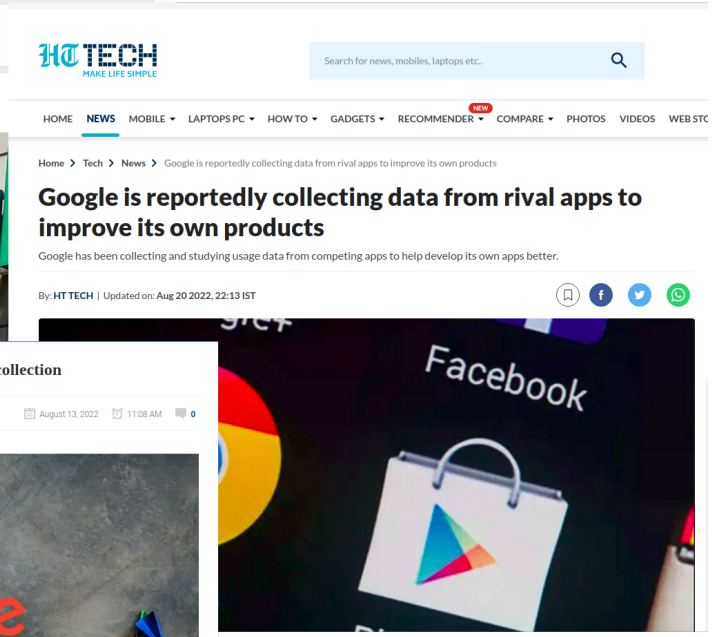
- In cryptography, there exists a special entity, called Adversary
  - Adversary tried to subvert what we are doing,
  - Tries to use our actions towards their advantage.
- A major part of cryptography deals with:
  - Understanding the intention and the behavior of the adversary,
  - Formalizing and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

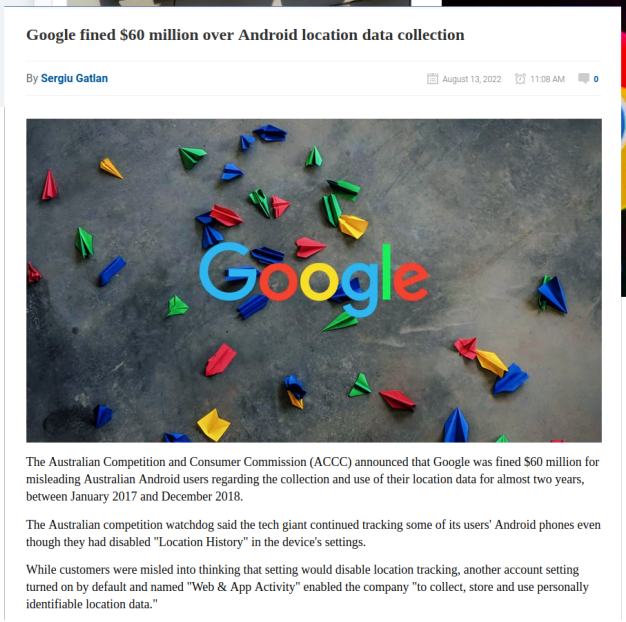
Adversaries are Everywhere



Adversaries are Everywhere







Adversaries are Everywhere

Figure: The Snowden Revelations

- 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.

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

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.

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.

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.

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

Doctor

Get Medical Record of SK

Medical Record of SK

Update the Medical Record of SK

Server of the Hogwarts Hospital

Security Goals Through Example

Doctor

Get Medical Record of SK

Medical Record of SK

Update the Medical Record of SK

Server of the Hogwarts Hospital

Ideal Scenario

- No Adversary,
- No Security Concern.

Security Goals Through Example

Doctor

Get Medical Record of SK

Medical Record of SK

Update the Medical Record of SK

Adversary

Server of the Hogwarts Hospital

Security Goals Through Example

Doctor

Get Medical Record of SK

Medical Record of SK

Update the Medical Record of SK

Adversary

Server of the Hogwarts Hospital

Privacy

- No one must learn about my medical condition.

Security Goals Through Example

Doctor

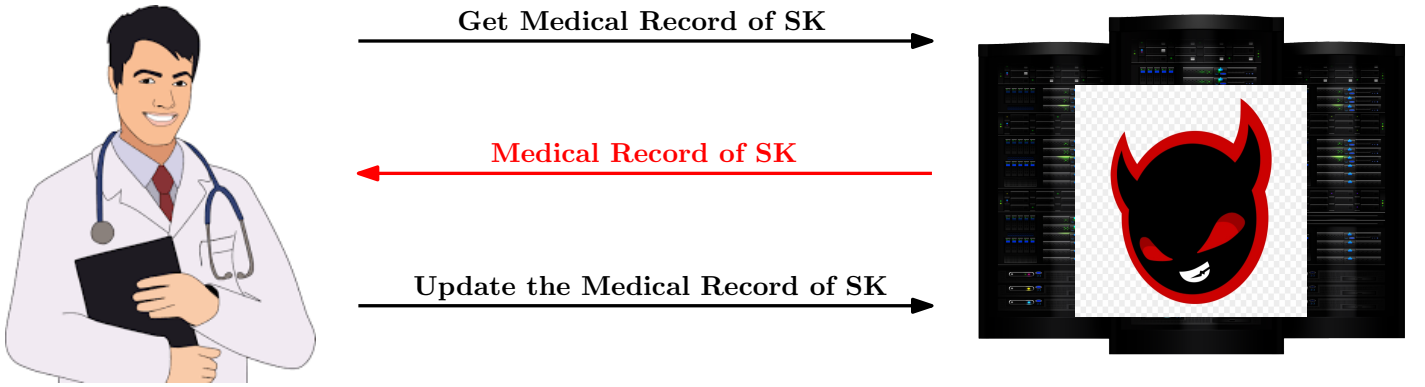
Get Medical Record of SK

Medical Record of SK

Update the Medical Record of SK

Server of the Hogwarts Hospital

Security Goals Through Example



Data Integrity

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

Security Goals Through Example

Doctor

Get Medical Record of SK

Medical Record of SK

Update the Medical Record of SK

Adversary

Security Goals Through Example

Doctor

Get Medical Record of SK

Medical Record of SK

Update the Medical Record of SK

Adversary

Authentication

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

Why is Privacy Important?

ELECTRONIC FRONTIER FOUNDATION

About Issues Our Work Take Action Tools Donate

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."**

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 | @germanrlopez | german.lopez@vox.com | Oct 13, 2014, 9:50am EDT

SHARE

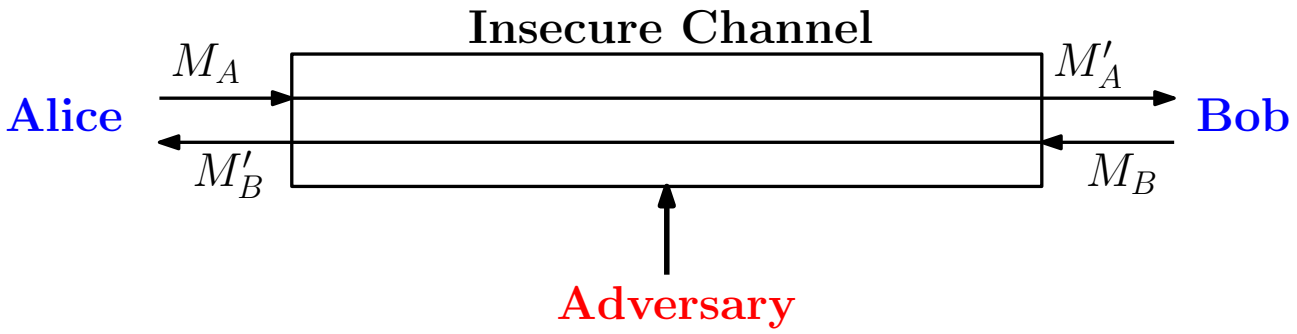
Greenwald has devised a challenge for people that tell him they don't worry about their privacy because they have nothing to hide: He asks them to send him all their email passwords and allow him to look through and publish anything he finds interesting. "After all, if you're not a bad person, if you're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

"All of us have things to hide," Greenwald said. "There are all sorts of things that we do and think that we're willing to tell our physician or our lawyer or our psychologist or our spouse or our best friend that we would be mortified for the rest of the world to learn."

Cryptography

Definition

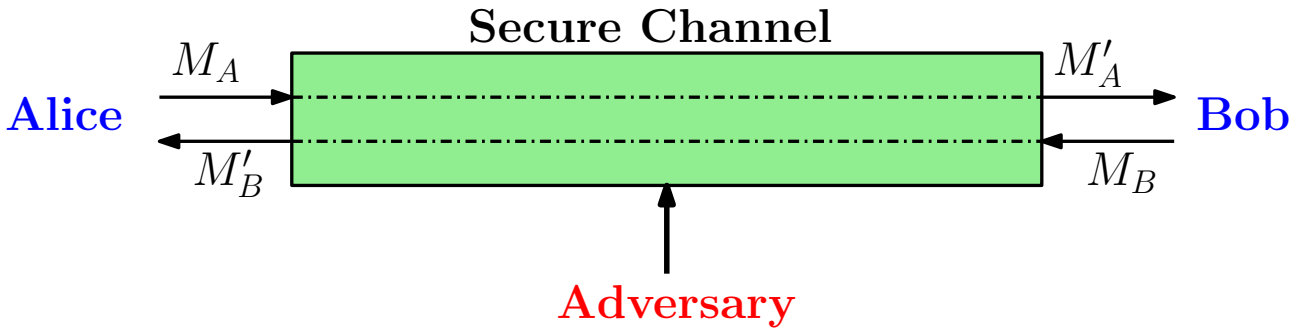
Cryptography is a means to enable parties to maintain privacy of the information they send to each other, even in the presence of an adversary with access to the communication channel.



Cryptography

Definition

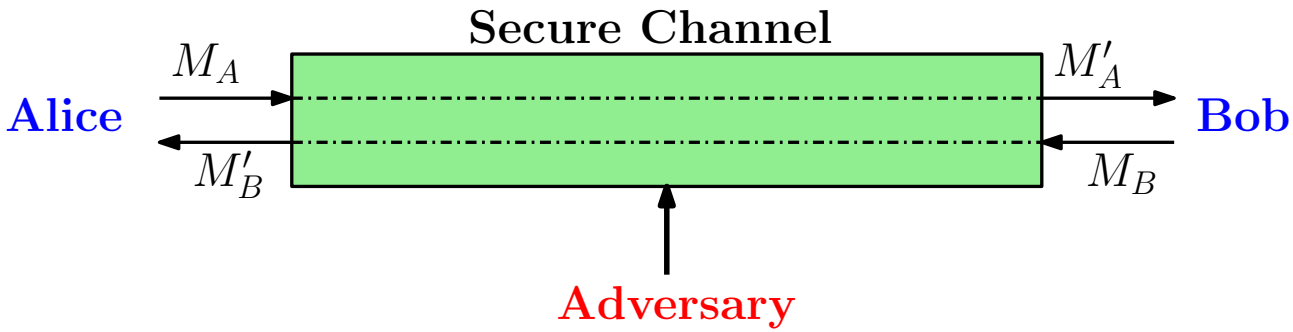
Cryptography is a means to enable parties to maintain privacy of the information they send to each other, even in the presence of an adversary with access to the communication channel.



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

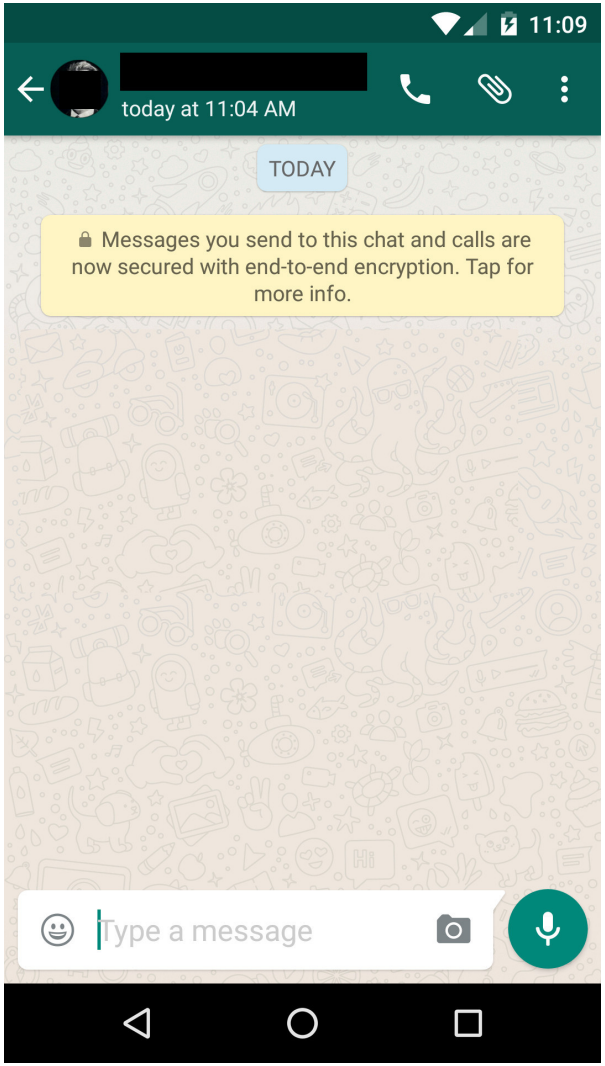


Figure: Whatsapp

Where do we use of Cryptography

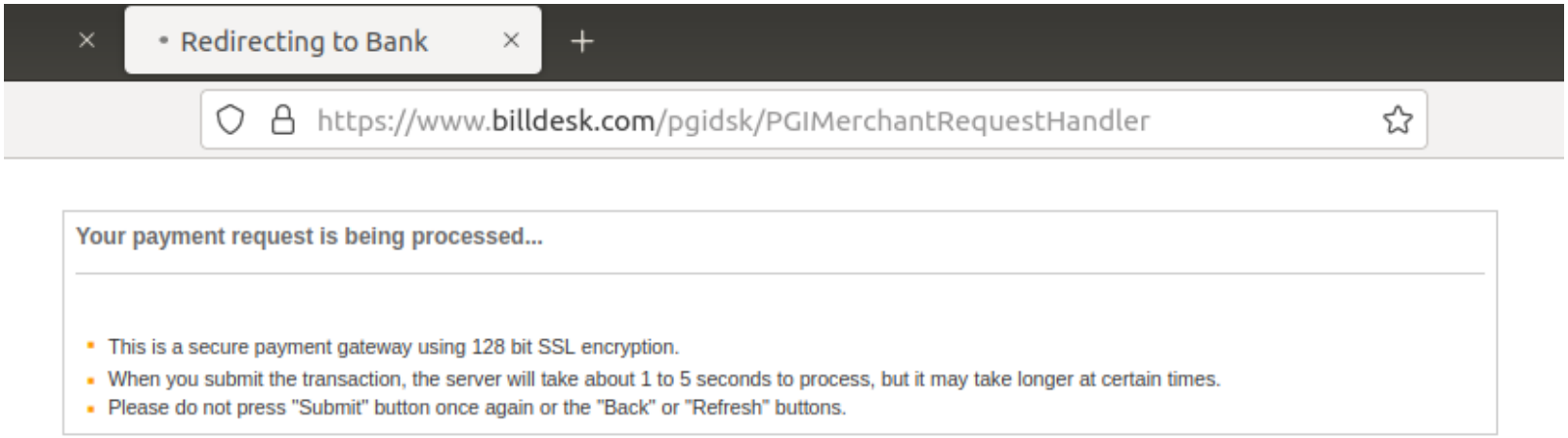


Figure: Billdesk Online Transaction

Where do we use of Cryptography

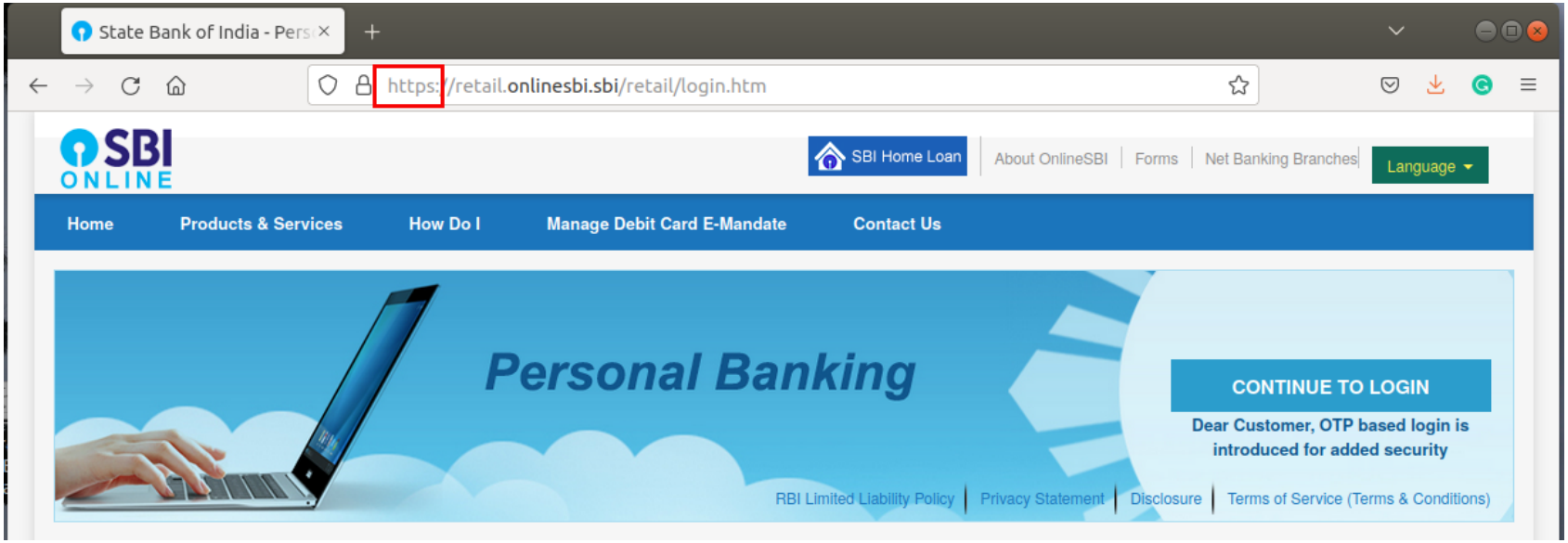


Figure: Transport Layer Security (TLS)

Where do we use of Cryptography

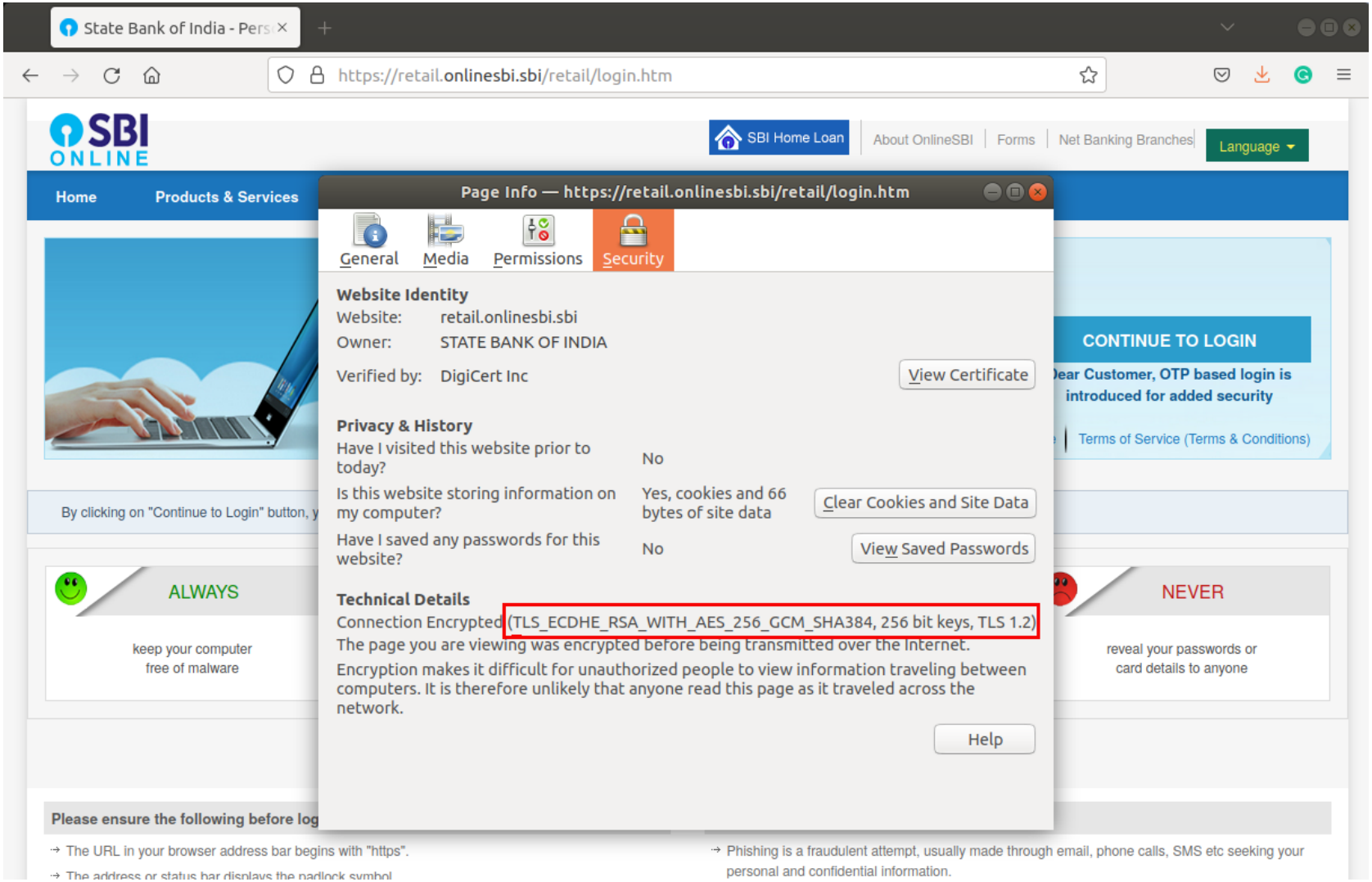
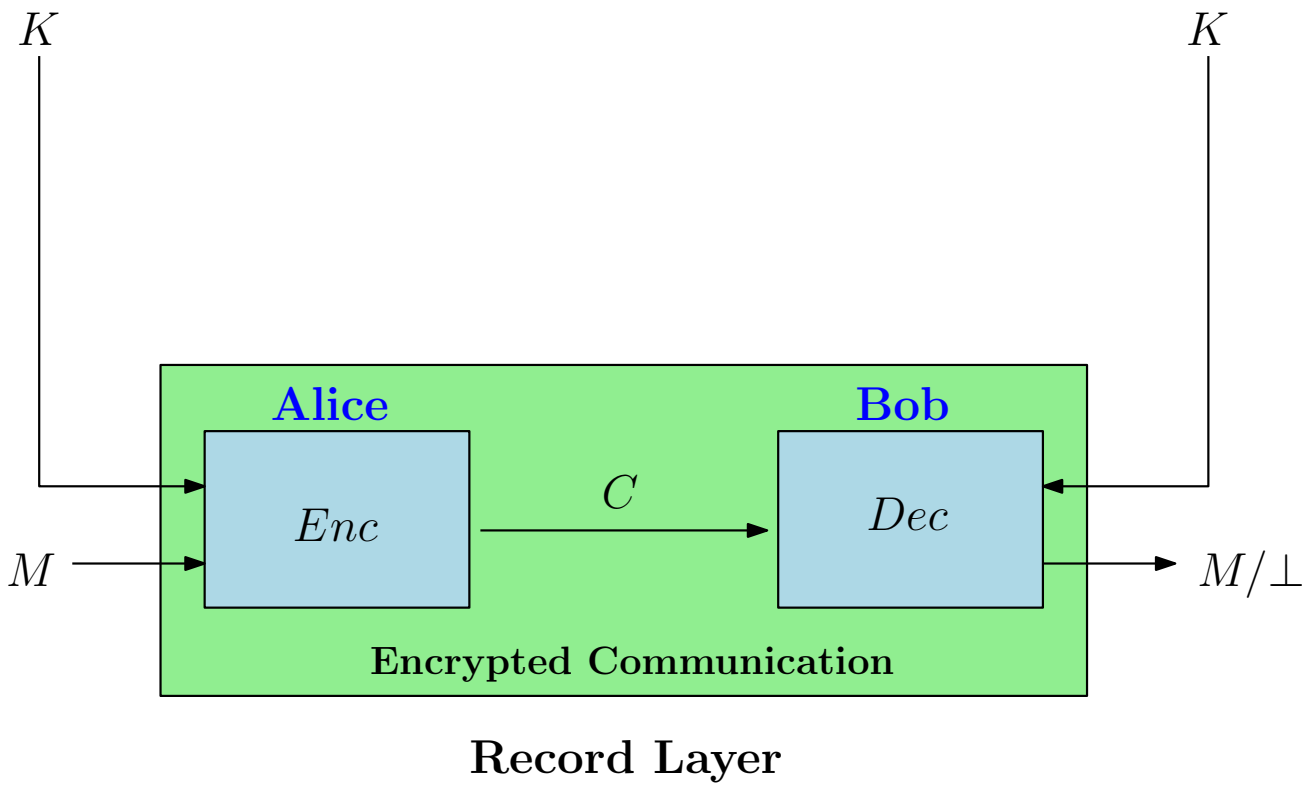


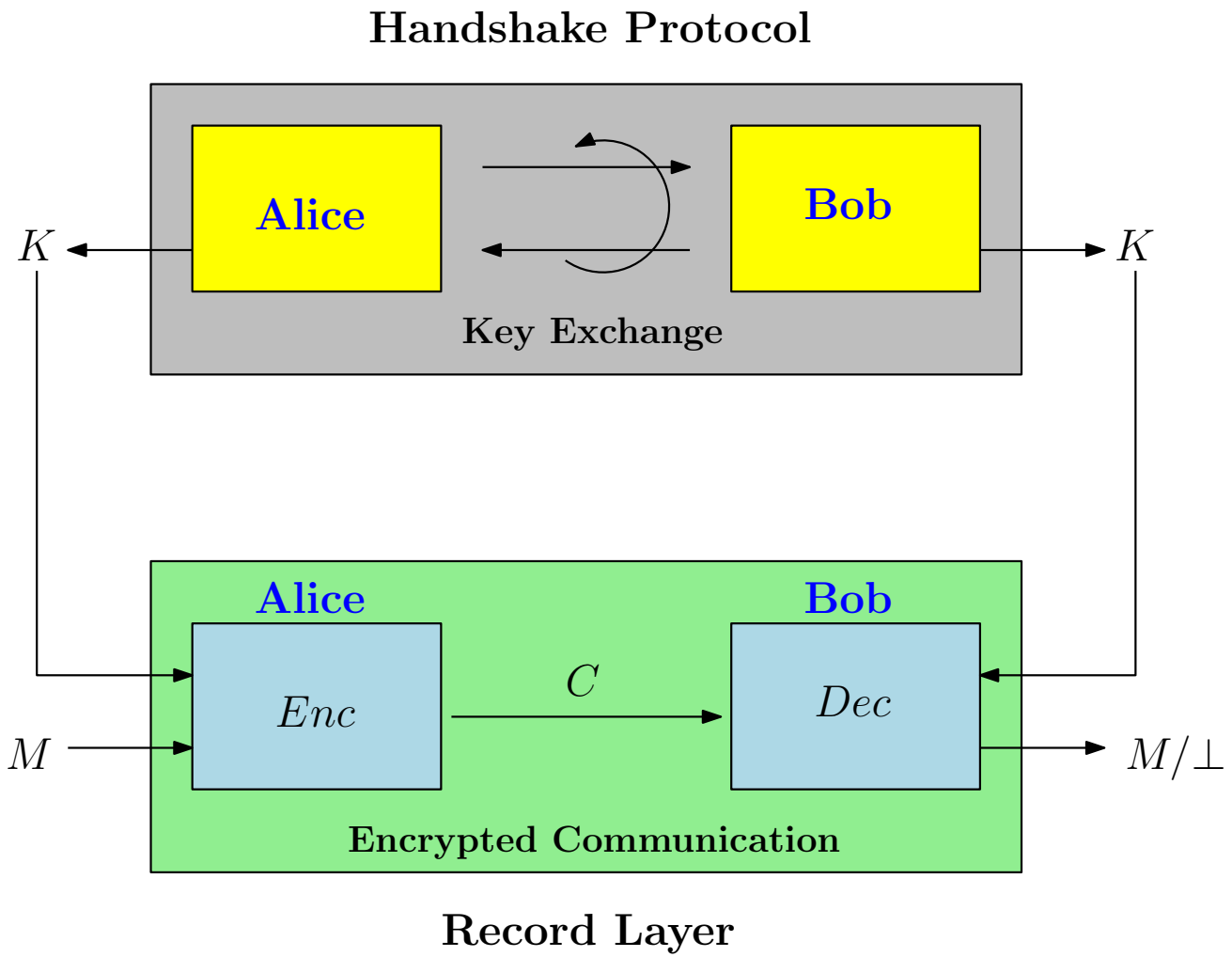
Figure: Transport Layer Security (TLS)

Basic of TLS/SSL

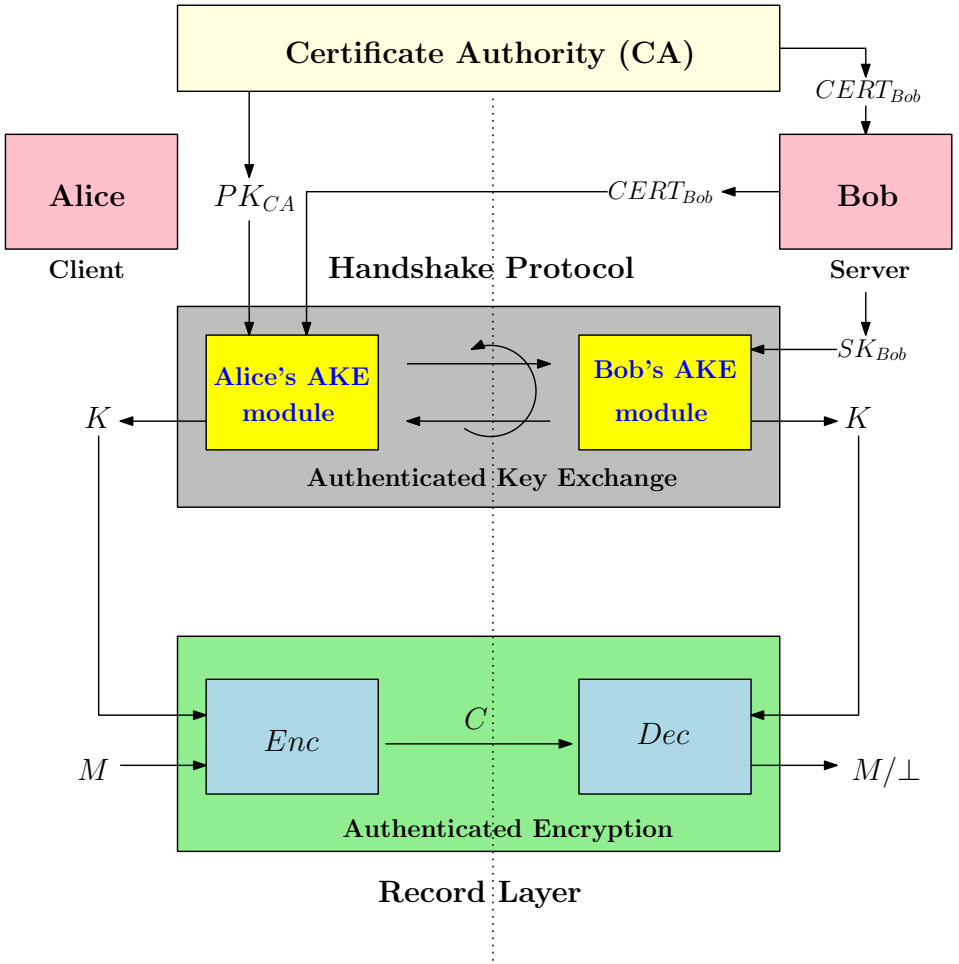


Record Layer

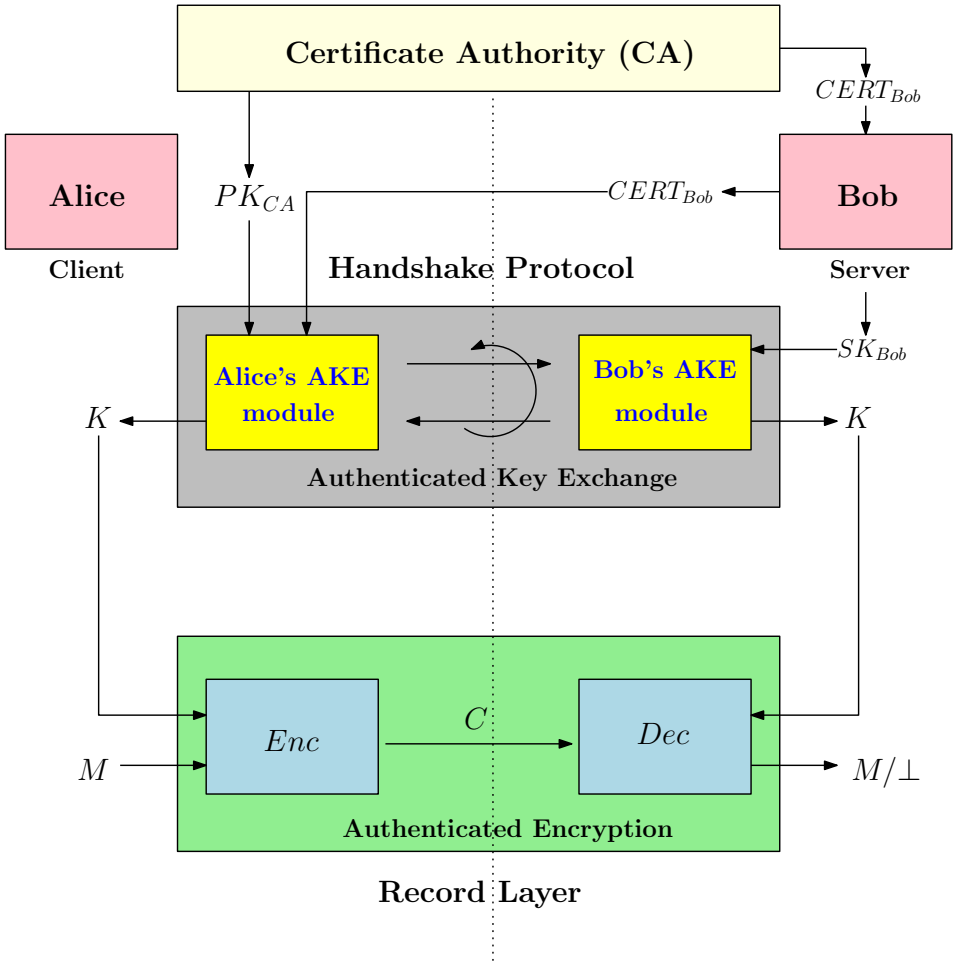
Basic of TLS/SSL



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 Sevice), 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.

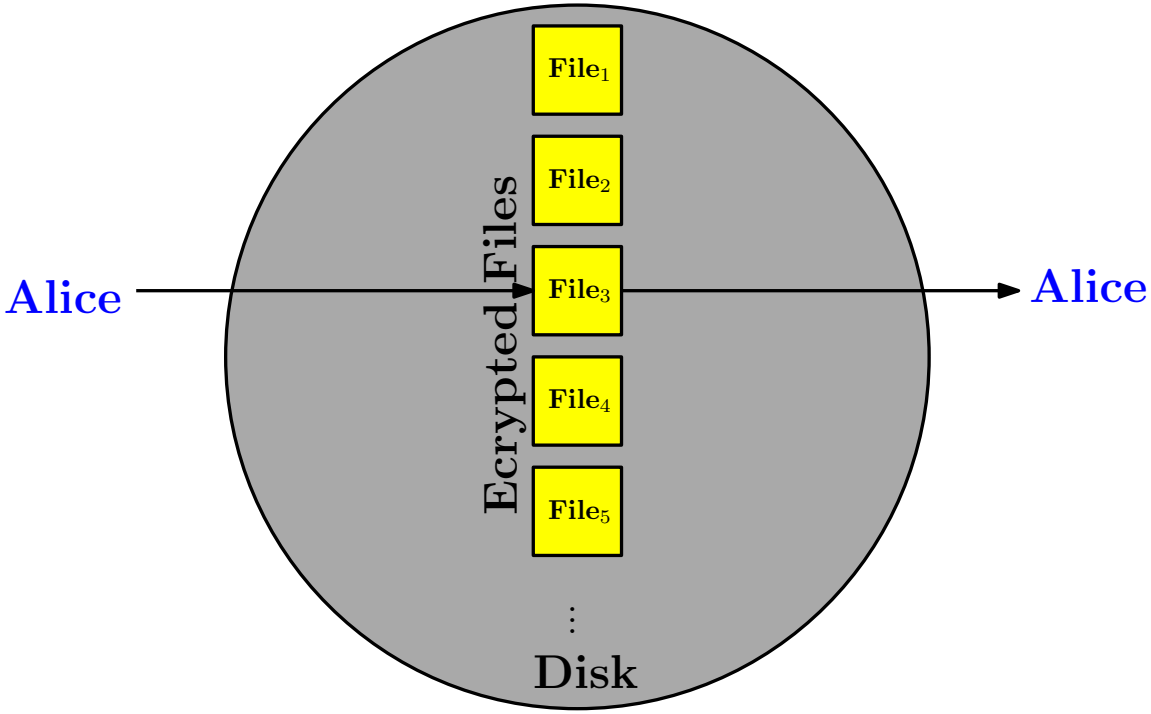
Vulnerabilities of TLS/SSL

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 Sevice), 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.
- Analogus 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

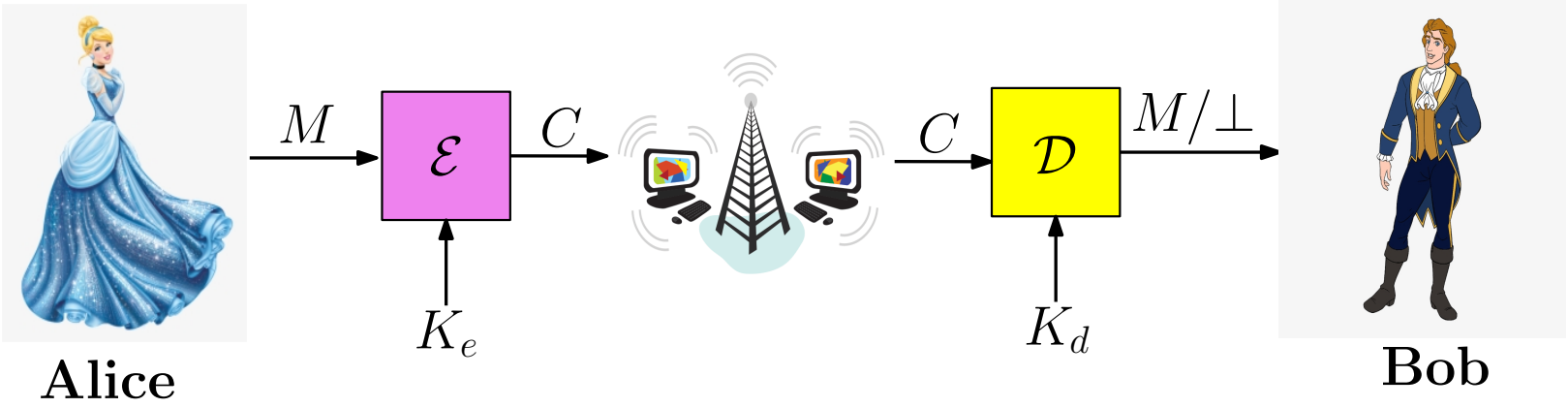
Cryptography is

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

Cryptography is not

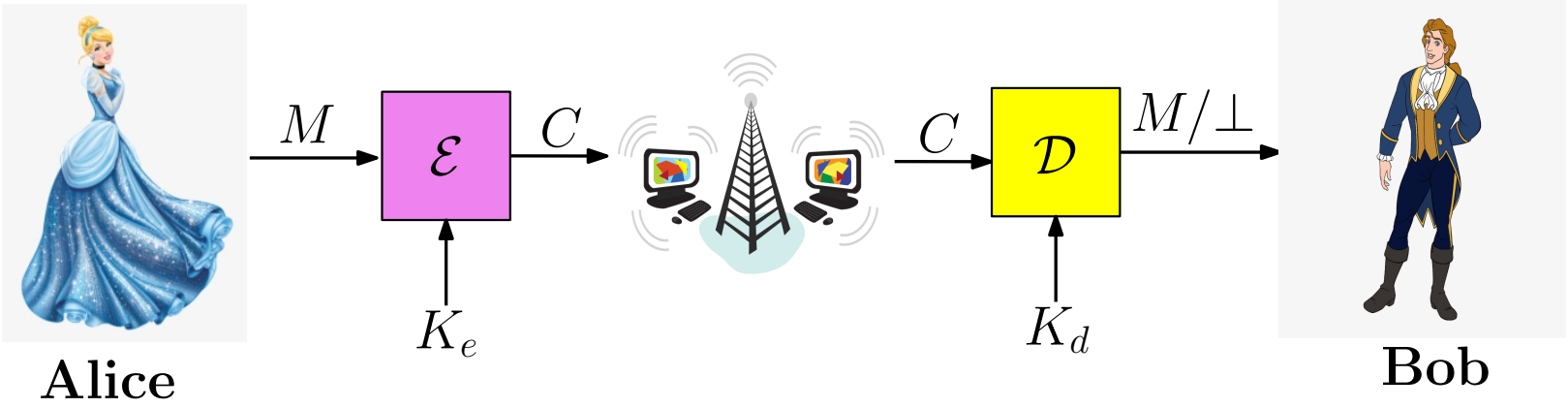
- Solution to every security problems.
- Reliable unless implemented and used properly.
- Something you should try to invent yourself: many many examples of broken ad-hoc designs.

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