CSL 505
CRYPTOGRAPHY

Welcome

Instructor
Dr. Dhiman Saha

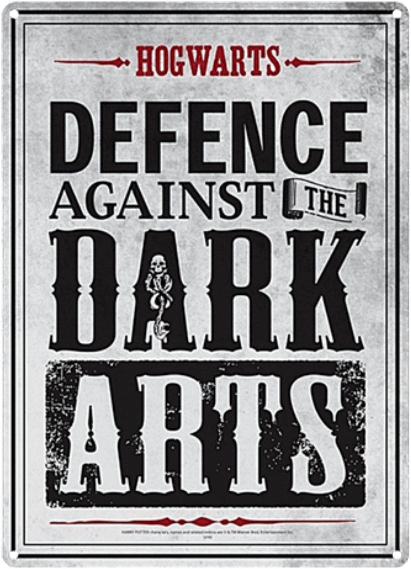


Image Source: Google

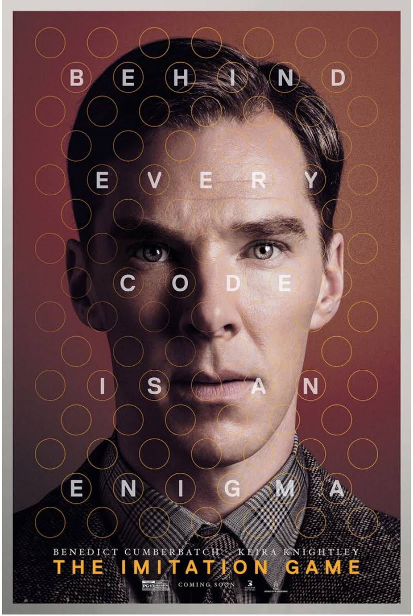


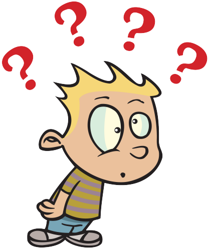
Image Source: Google

CSL 505

CRYPTOGRAPHY

Instructor
Dr. Dhiman Saha

CANVAS



- What is Crypto?
- Why is it needed?
- Why should I study it?
- Is it difficult?
- Will I pass?

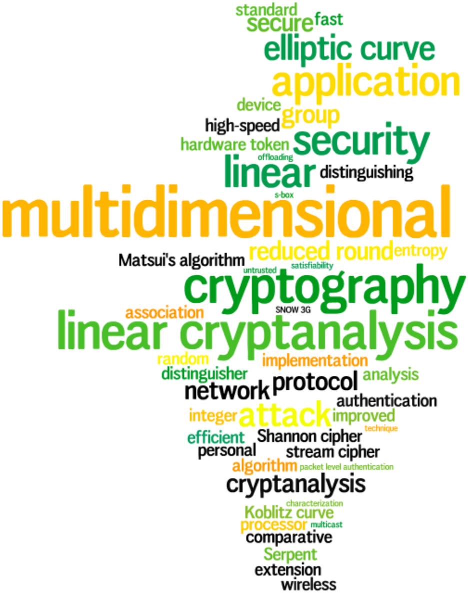
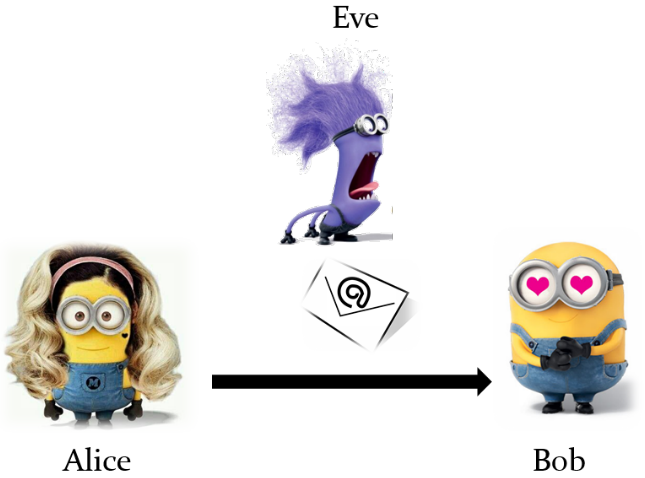


Image Credits: Crypto Group Alto University

The Story of Alice and Bob

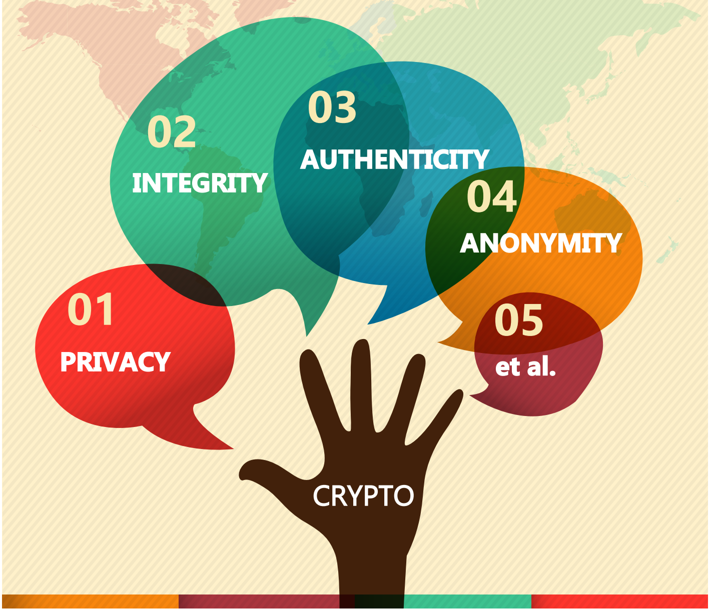


Eve

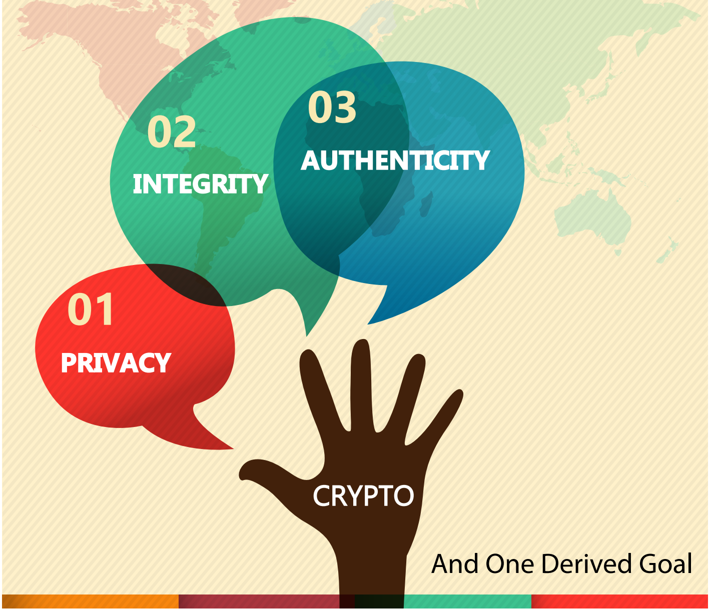
Alice

Bob

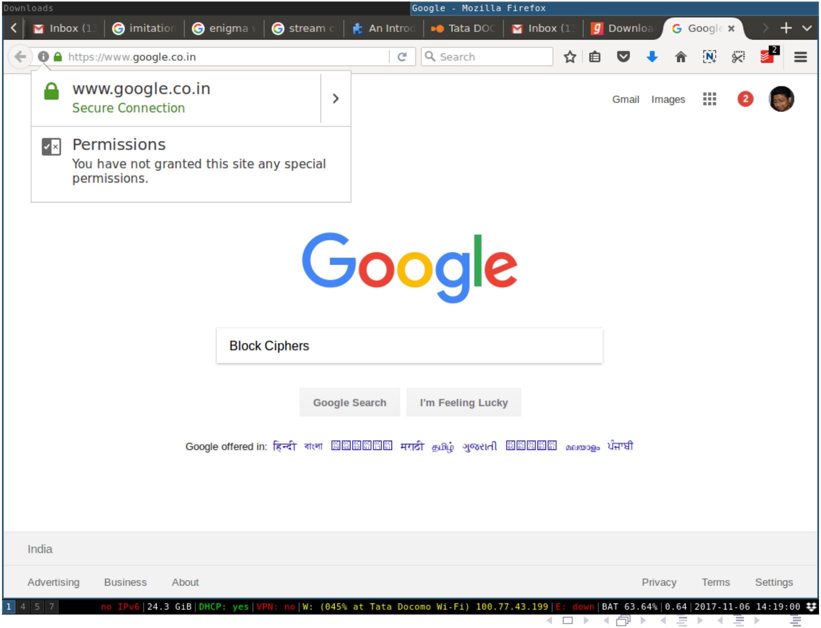
Cryptographic Goals



Our Focus


01
PRIVACY
02
INTEGRITY
03
AUTHENTICITY
CRYPTO
And One Derived Goal

Your Favourite Search Engine Uses HTTPS



https://www.google.co.in

www.google.co.in
Secure Connection

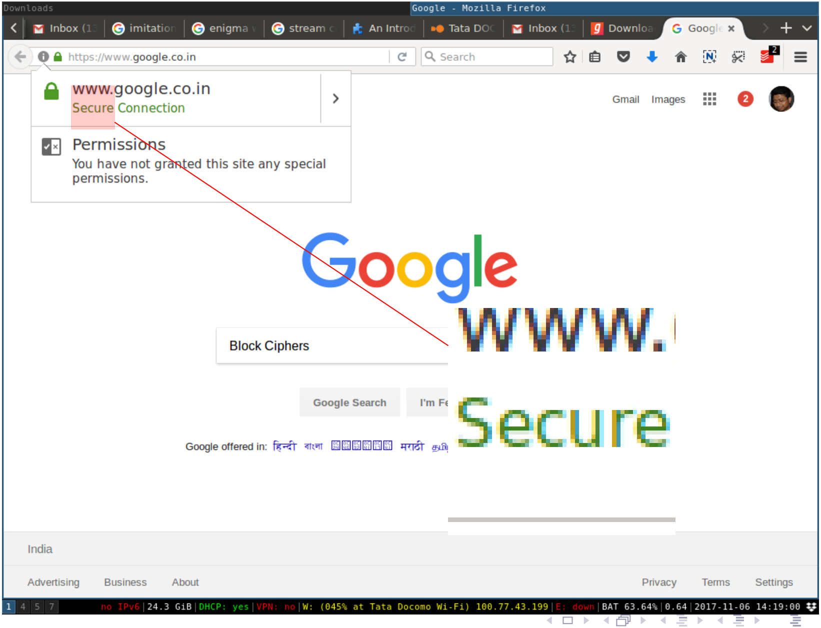
Permissions
You have not granted this site any special permissions.

Block Ciphers

Google offered in: हिन्दी বাংলা मराठी தமிழ் ગુજરાતી മലയാളം ਪੰਜਾਬੀ

```
1 4 5 7   no IPv6|24.3 GiB|DHCP: yes|VPN: no|W: (045% at Tata Docomo Wi-Fi) 100.77.43.199|E: down|BAT 63.64%|0.64|2017-11-06 14:19:00
```

Your Favourite Search Engine Uses HTTPS



Google - Mozilla Firefox

https://www.google.co.in

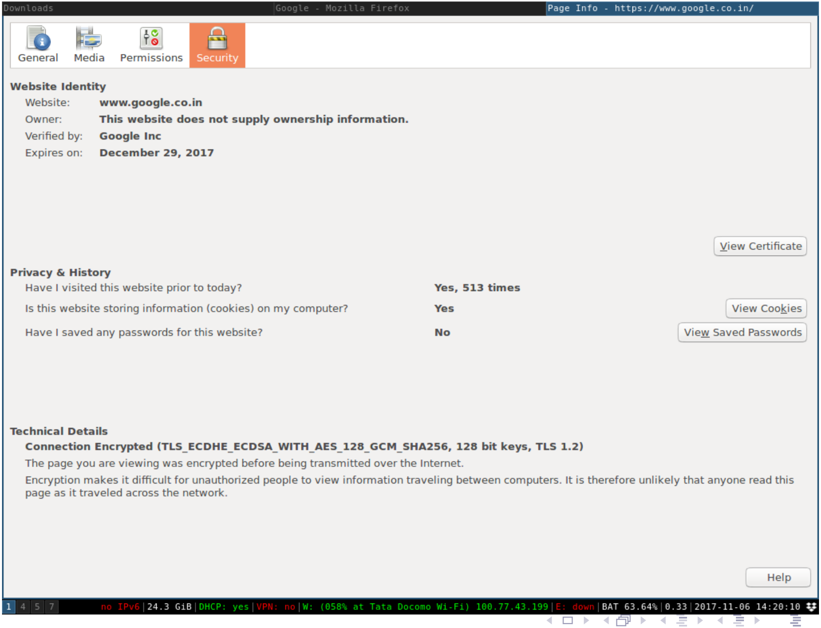
www.google.co.in
Secure Connection

Permissions
You have not granted this site any special permissions.

Block Ciphers

```
1 4 5 7   no IPv6 | 24.3 GiB | DHCP: yes | VPN: no | W: (045% at Tata Docomo Wi-Fi) 100.77.43.199 | E: down | BAT 63.64% | 0.64 | 2017-11-06 14:19:00
```

Behind the scenes https://www.google.co.in



Website Identity

Website: **www.google.co.in**

Owner: **This website does not supply ownership information.**

Verified by: **Google Inc**

Expires on: **December 29, 2017**

Privacy & History

Have I visited this website prior to today?	**Yes, 513 times**
Is this website storing information (cookies) on my computer?	**Yes**
Have I saved any passwords for this website?	**No**

Technical Details

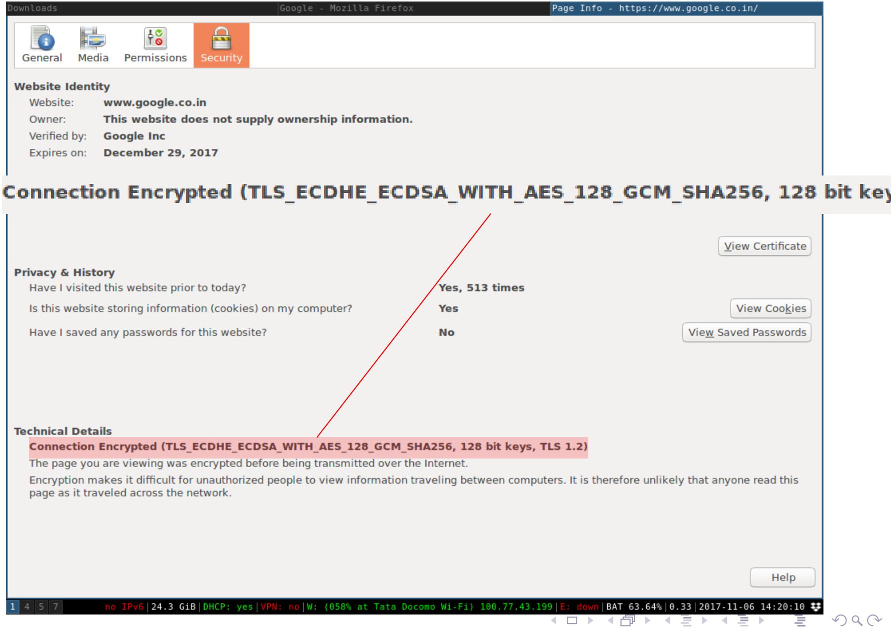
Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

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.

```
no IPv6|24.3 GiB|DHCP: yes|VPN: no|W: (058% at Tata Docomo Wi-Fi) 100.77.43.199|E: down|BAT 63.64%|0.33|2017-11-06 14:20:10
```

Behind the scenes https://www.google.co.in



Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit key

Website Identity

Website: **www.google.co.in**
Owner: **This website does not supply ownership information.**
Verified by: **Google Inc**
Expires on: **December 29, 2017**

Privacy & History

Have I visited this website prior to today? **Yes, 513 times**
Is this website storing information (cookies) on my computer? **Yes**
Have I saved any passwords for this website? **No**

Technical Details

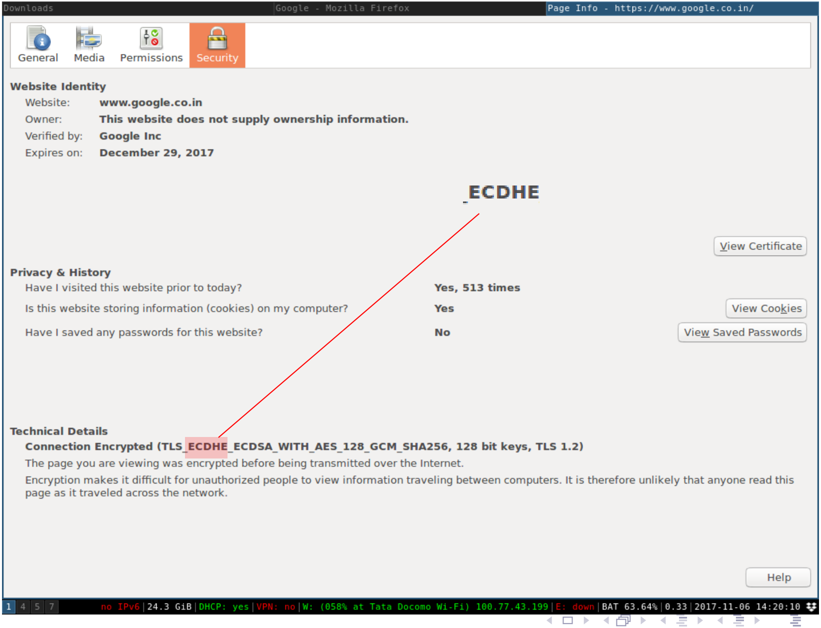
Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

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.

```
1 4 5 7   no IPv6|24.3 GiB|DHCP: yes|VPN: no|W: (058% at Tata Docomo Wi-Fi) 100.77.43.199|E: down|BAT 63.64%|0.33|2017-11-06 14:20:10
```

Key-Exchange Mechanism



Website Identity

Website: **www.google.co.in**

Owner: **This website does not supply ownership information.**

Verified by: **Google Inc**

Expires on: **December 29, 2017**

_ECDHE

Privacy & History

Have I visited this website prior to today? **Yes, 513 times**

Is this website storing information (cookies) on my computer? **Yes**

Have I saved any passwords for this website? **No**

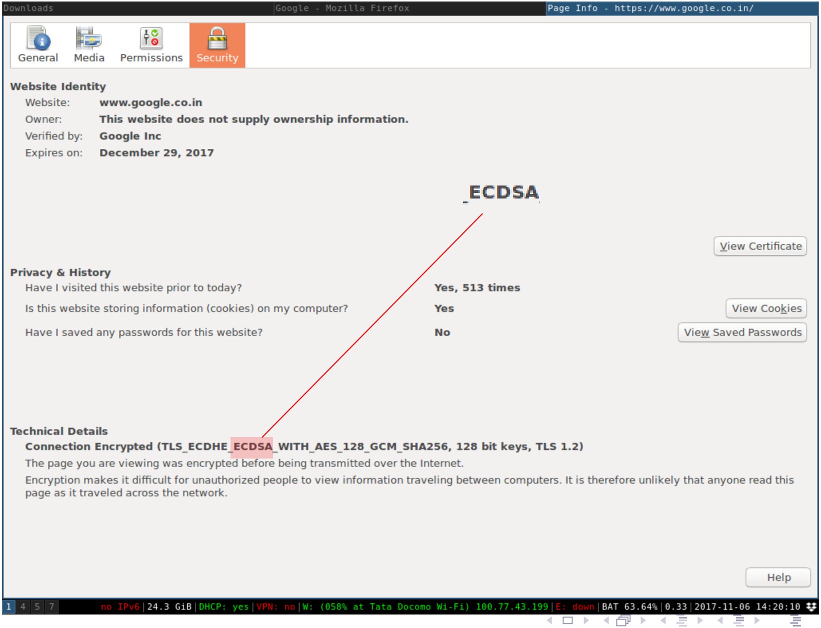
Technical Details

Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 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.

```
1 4 5 7   no IPv6|24.3 GiB|DHCP: yes|VPN: no|W: (058% at Tata Docomo Wi-Fi) 100.77.43.199|E: down|BAT 63.64%|0.33|2017-11-06 14:20:10
```



Website Identity

Website: **www.google.co.in**

Owner: **This website does not supply ownership information.**

Verified by: **Google Inc**

Expires on: **December 29, 2017**

_ECDSA

Privacy & History

Have I visited this website prior to today?	**Yes, 513 times**	
Is this website storing information (cookies) on my computer?	**Yes**	View Cookies
Have I saved any passwords for this website?	**No**	View Saved Passwords

Technical Details

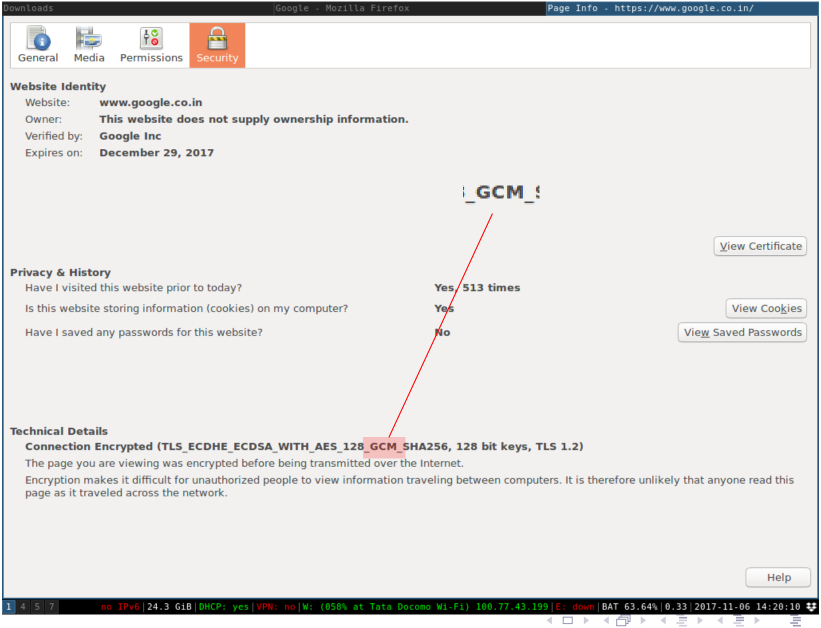
Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

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.

```
1 4 5 7   no IPv6|24.3 GiB|DHCP: yes|VPN: no|W: (058% at Tata Docomo Wi-Fi) 100.77.43.199|E: down|BAT 63.64%|0.33|2017-11-06 14:20:10
```

GCM Authenticated Encryption Scheme



Downloads
Google - Mozilla Firefox
Page Info - https://www.google.co.in/
General
Media
Permissions
Security
GCM
View Certificate
View Cookies
View Saved Passwords
Help
1 4 5 7
no IPv6 | 24.3 GiB | DHCP: yes | VPN: no | W: (058% at Tata Docomo Wi-Fi) 100.77.43.199 | E: down | BAT 63.64% | 0.33 | 2017-11-06 14:20:10

Website Identity

Website: **www.google.co.in**

Owner: **This website does not supply ownership information.**

Verified by: **Google Inc**

Expires on: **December 29, 2017**

Privacy & History

Have I visited this website prior to today? **Yes, 513 times**

Is this website storing information (cookies) on my computer? **Yes**

Have I saved any passwords for this website? **No**

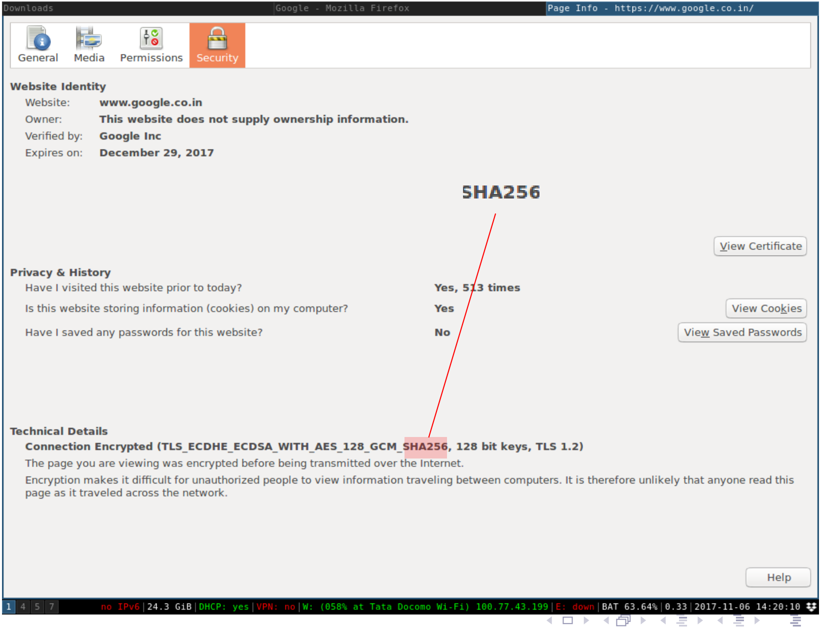
Technical Details

Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 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.

SHA256



Website Identity

Website: **www.google.co.in**

Owner: **This website does not supply ownership information.**

Verified by: **Google Inc**

Expires on: **December 29, 2017**

SHA256

Privacy & History

Have I visited this website prior to today? **Yes, 513 times**

Is this website storing information (cookies) on my computer? **Yes**

Have I saved any passwords for this website? **No**

Technical Details

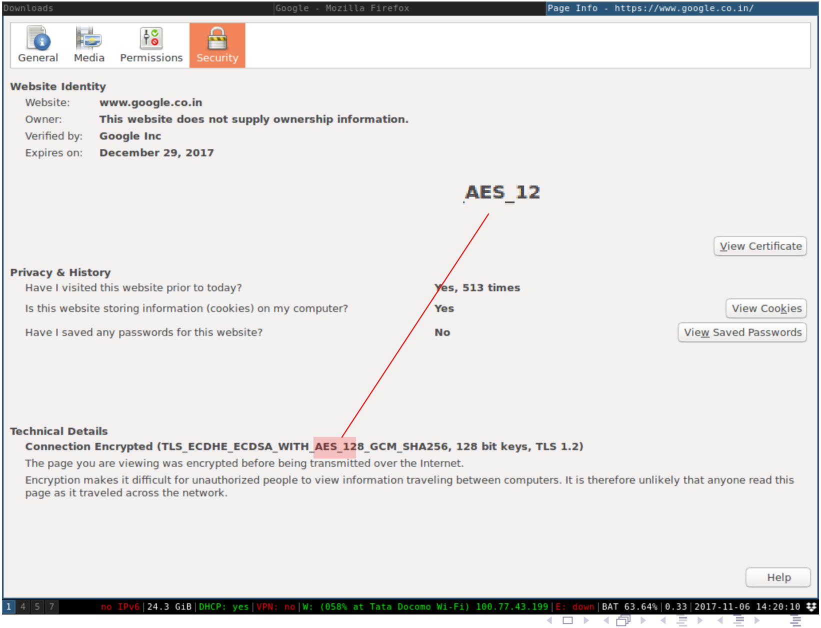
Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

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.

```
1 4 5 7   no IPv6|24.3 GiB|DHCP: yes|VPN: no|W: (058% at Tata Docomo Wi-Fi) 100.77.43.199|E: down|BAT 63.64%|0.33|2017-11-06 14:20:10
```

AES Block Cipher


Downloads
Google - Mozilla Firefox
Page Info - https://www.google.co.in/
General
Media
Permissions
Security
AES_12
View Certificate
View Cookies
View Saved Passwords
Help
1 4 5 7
no IPv6 | 24.3 GiB | DHCP: yes | VPN: no | W: (058% at Tata Docomo Wi-Fi) 100.77.43.199 | E: down | BAT 63.64% | 0.33 | 2017-11-06 14:20:10

Website Identity

Website: **www.google.co.in**

Owner: **This website does not supply ownership information.**

Verified by: **Google Inc**

Expires on: **December 29, 2017**

Privacy & History

Have I visited this website prior to today? **Yes, 513 times**

Is this website storing information (cookies) on my computer? **Yes**

Have I saved any passwords for this website? **No**

Technical Details

Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

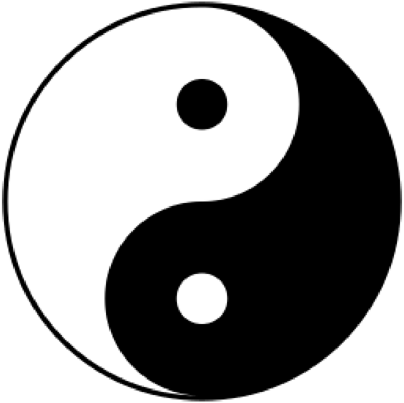
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Kerchoffs's Principle

By Dutch cryptographer
Auguste Kerckhoffs

Everything about a cryptosystem, **except the key**, is public knowledge

- ~~Security through obscurity~~
- However, some parameter must be **secret**
  - Known only to authorized entities: Alice, Bob
  - That parameter is the "key"
  - Distinguishes between Bob and Eve



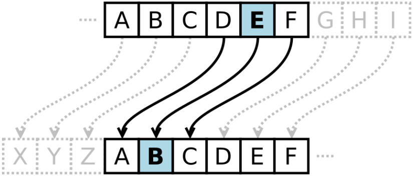
Yin and Yang

Cryptography
&
Cryptanalysis

Historical Cipher

Caesar (Shift) Cipher

- One of the earliest known ciphers
- Special case of substitution
- Shifts the letters by a constant number
- Allegedly used by Julius Caesar using a shift of 3



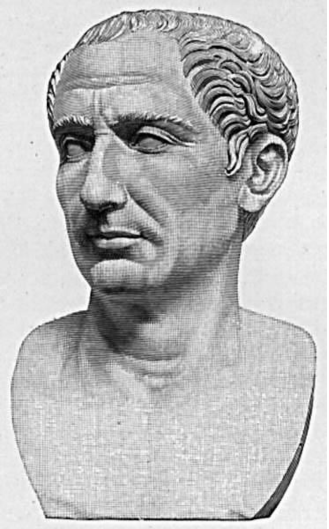


Image Credits: Wikipedia

- Applies **modular arithmetic**
- Letter ↔ number translation

$$a \to 0, b \to 1, c \to 2, \cdots, z \to 25$$

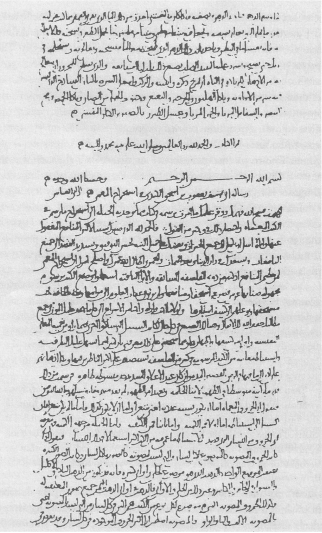
Encryption

$$e(x) = (x + k) \mod 26$$

Decryption

$$d(x) = (x - k) \mod 26$$

- How many possible keys?
- Notion of brute-force attack
- Can we break it without guessing the key?
- What if the key-space was "**huge**" ?



The first page of al-Kindi's manuscript
On Deciphering Cryptographic Messages

- Earliest reference on code-breaking
- 9th Century Arab scientist - **al-Kindi**
- Rediscovered in 1987 in Istanbul

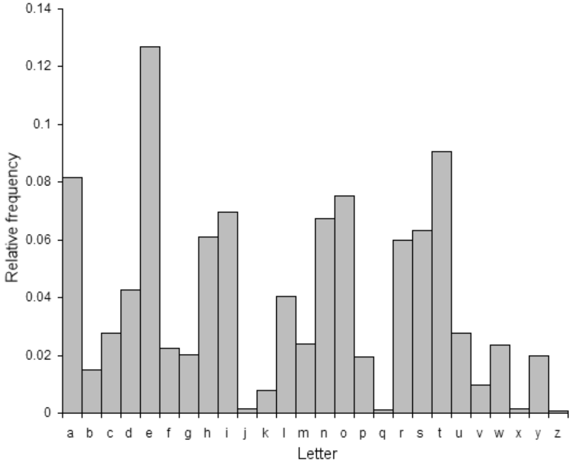
A Manuscript on Deciphering Encrypted Messages

- Explores idea of output preserving input statistics
- For e.g. letter frequency analysis

Ref. The History of Cryptography-Simon Singh

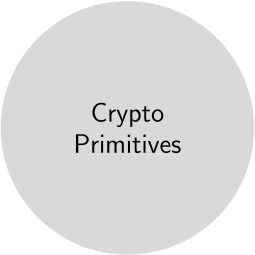
Frequency Analysis

English Letter Frequencies



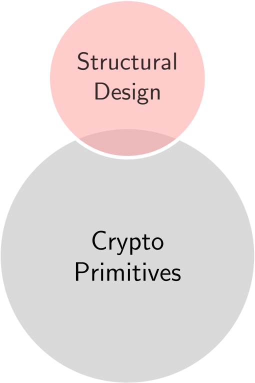
- Can be used to break Caesar Cipher. How?

Course Approach — Four Dimensional

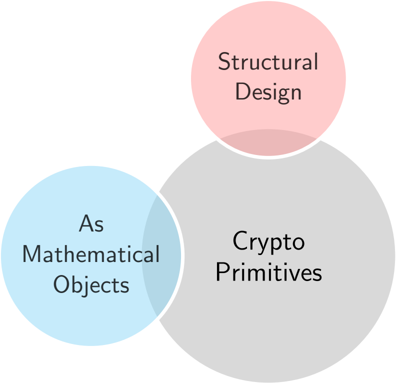


Crypto
Primitives

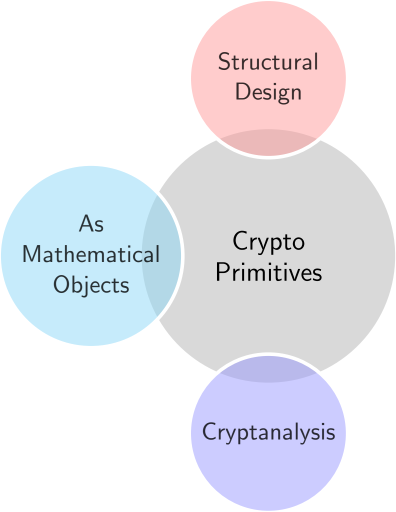
Course Approach — Four Dimensional



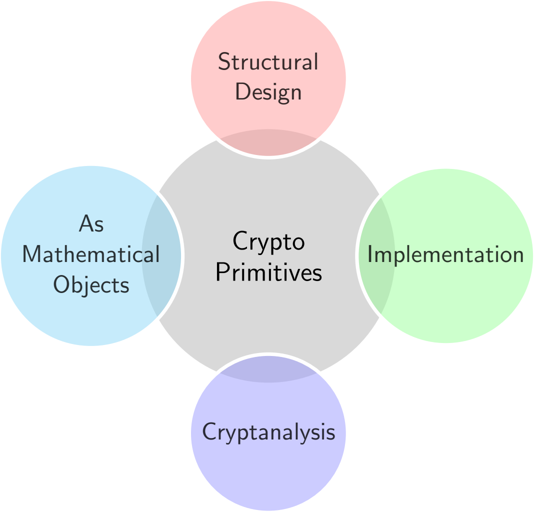
Course Approach Four Dimensional



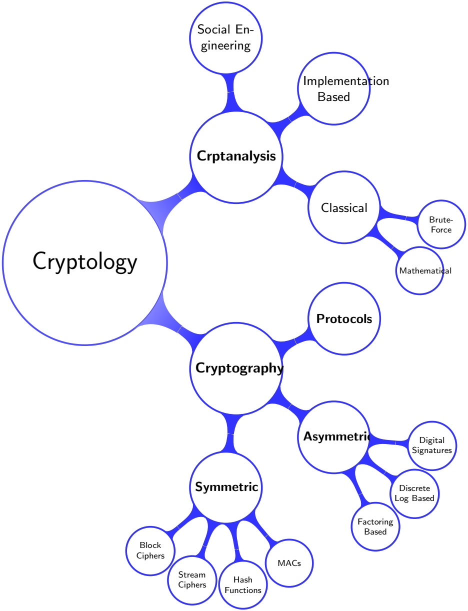
Course Approach Four Dimensional



Course Approach Four Dimensional



Crypto at a glance! Rough Taxonomy



Home Assignment - Group Submission

- Find a historical cipher (say one that was used before 1980's)
- You will get extra marks if your cipher is unique.
- Some of them will be highlighted in next class.

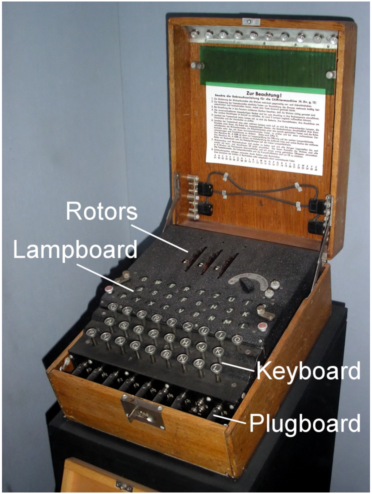
Note

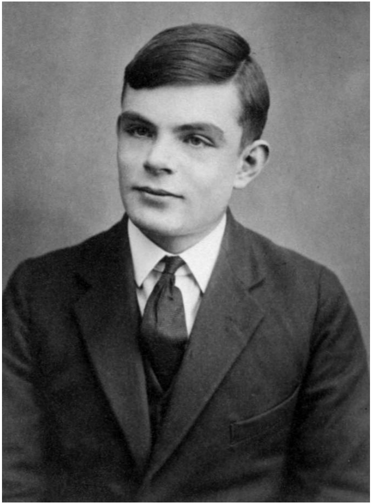
Shift-Cipher and Enigma are already taken.

Books/References

- Cryptography: Theory and Practice by Douglas R. Stinson.
- Understanding Cryptography by Christof Paar and Jan Pelzl
- Other references will be shared as and when required

Enigma!





See you in next class.

Image Credits: Wikipedia