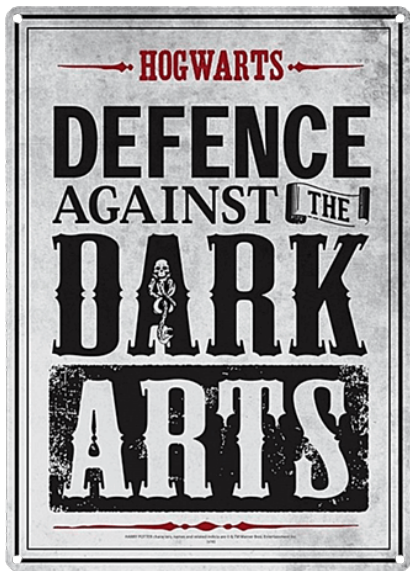
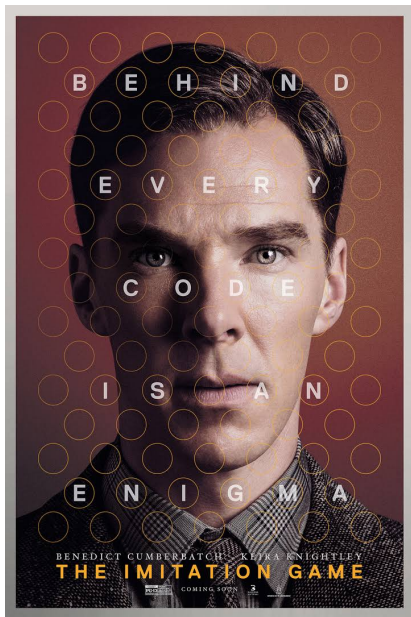


CS 553

CRYPTOGRAPHY

Instructor
Dr. Dhiman Saha



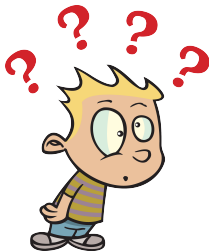


CS 553

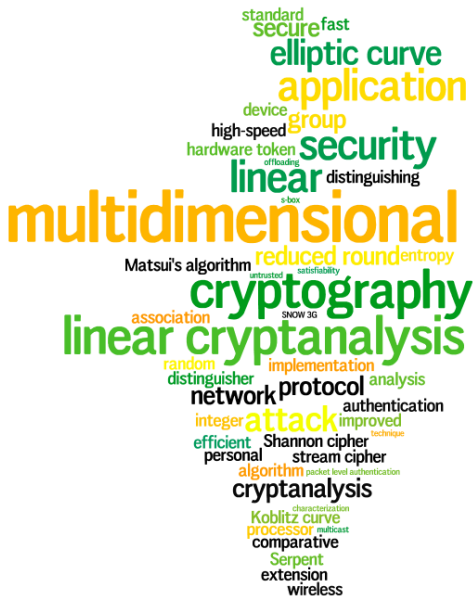
CRYPTOGRAPHY

Instructor
Dr. Dhiman Saha

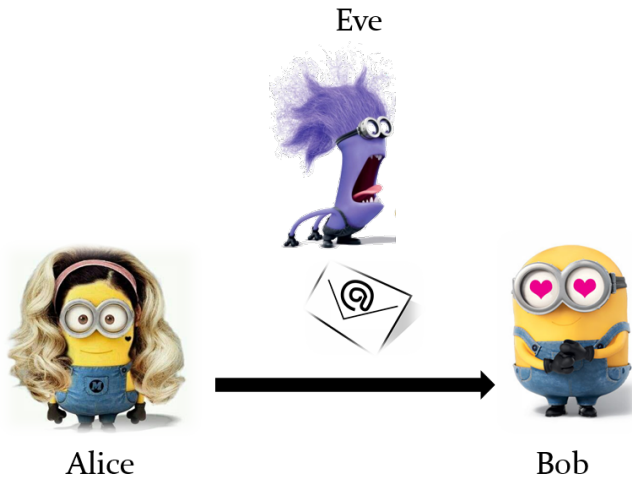




- ▶ What is Crypto?
- ▶ Why is it needed?
- ▶ Why should I study it?
- ▶ Is it difficult?
- ▶ Will I pass?

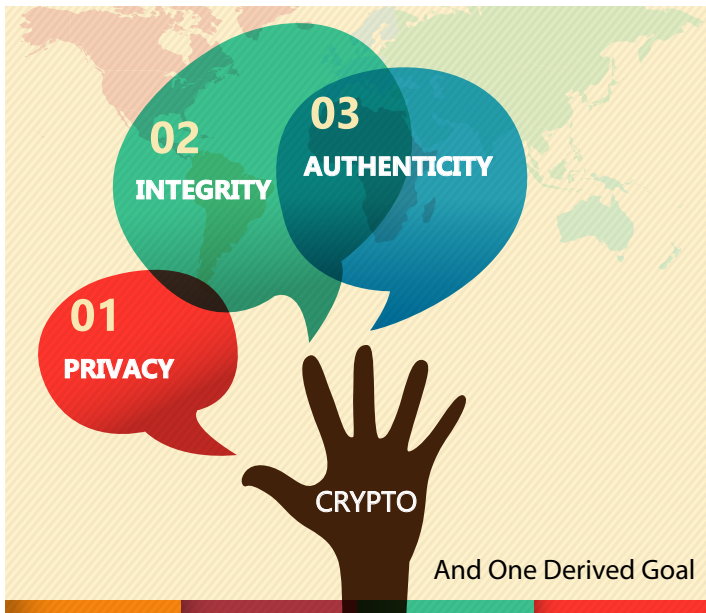


The Story of Alice and Bob



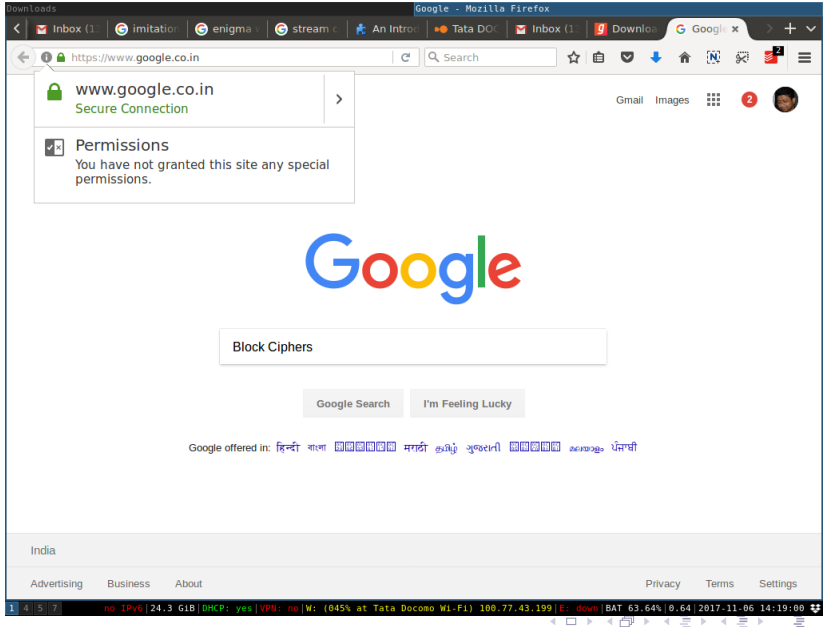
Cryptographic Goals





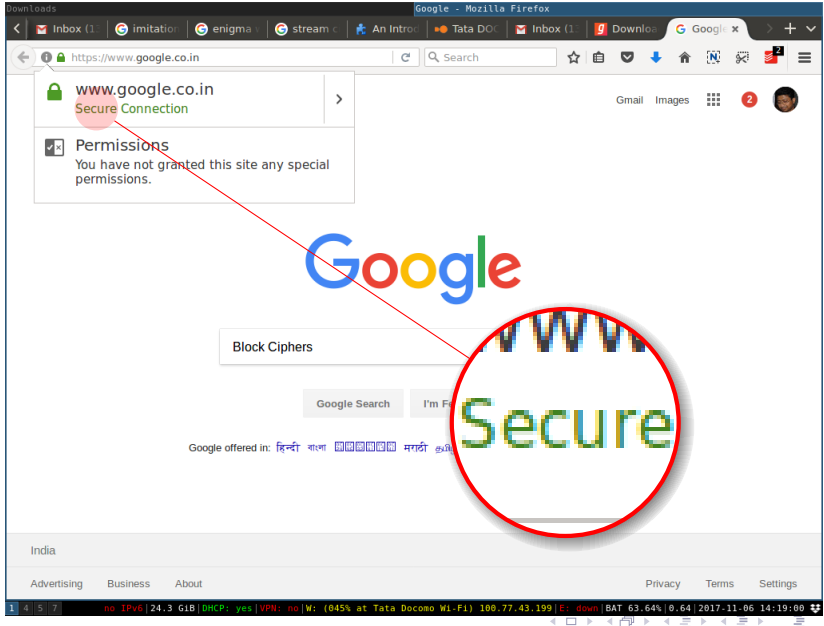
Your Favourite Search Engine

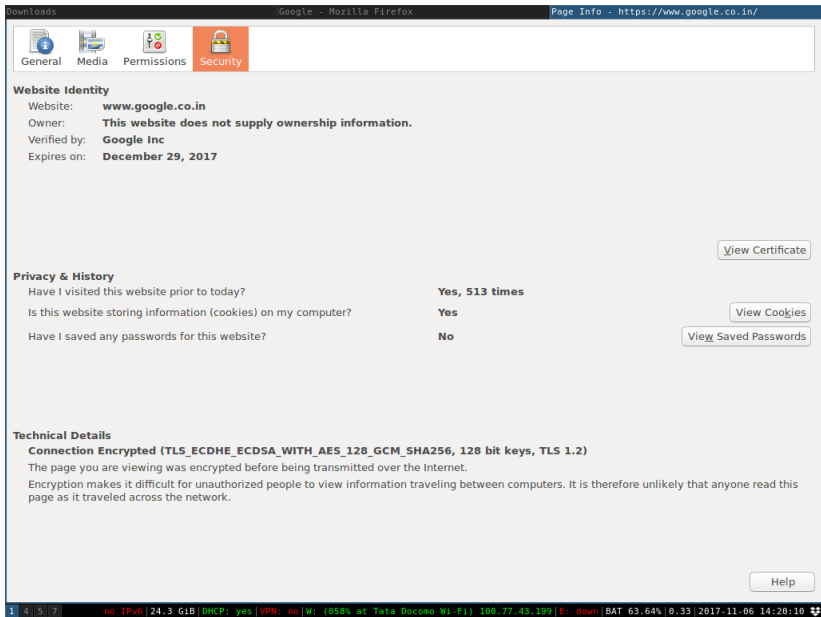
Uses HTTP**S**



Your Favourite Search Engine

Uses HTTPS





The screenshot shows the 'Page Info' window in Mozilla Firefox. The window title is 'Page Info - https://www.google.co.in/'. The window has a toolbar with icons for General, Media, Permissions, and Security. The 'Security' tab is selected, showing the following information:

Website Identity

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

[View Certificate](#)

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.

[Help](#)

At the bottom of the window, there is a status bar showing the following information: 1 4 5 7 no IPv6 | 24.3 G1B | 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

Downloads Google - Mozilla Firefox Page Info - <https://www.google.co.in/>

General Media Permissions **Security**

Website Identity

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

Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit key)

[View Certificate](#)

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.

[Help](#)

1 4 5 7 no IPv6 | 24.3 G1B | 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

The screenshot shows the Firefox browser's Security tab for the URL <https://www.google.co.in/>. The browser's address bar shows "Google - Mozilla Firefox" and "Page Info - https://www.google.co.in/". The Security tab is active, displaying icons for General, Media, Permissions, and Security. The "Website Identity" section shows the website is **www.google.co.in**, owned by **Google Inc**, and expires on **December 29, 2017**. The "Privacy & History" section shows the user has visited the site 513 times, and it is storing cookies and saved passwords. The "Technical Details" section shows the connection is encrypted using **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2**. A red box highlights the text "ECDHE" in the "Technical Details" section, and a red line connects it to the "ECDHE" text in the "Website Identity" section. The status bar at the bottom shows network information: "no IPv6 | 24.3 G1B | DHCP: yes | VPN: no | W: (058% at Tata Decomo 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**

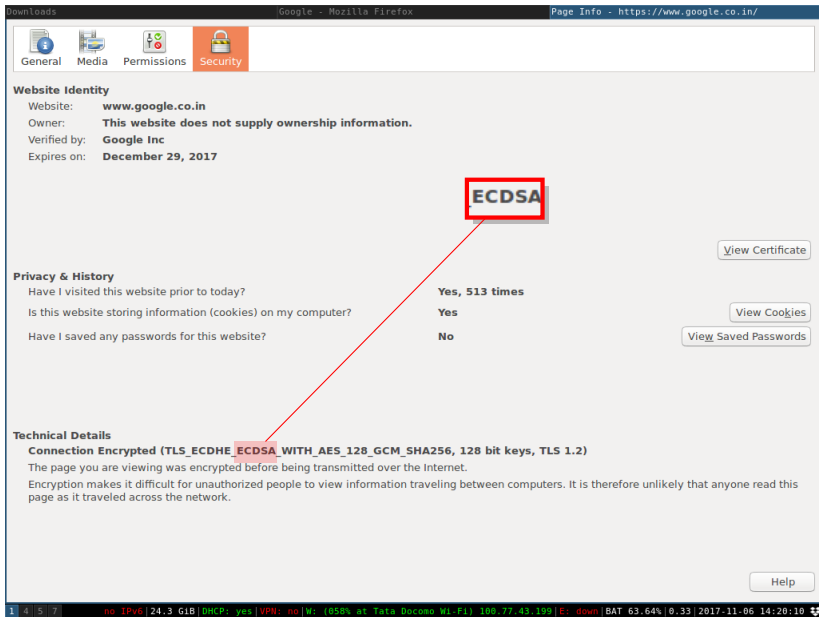
Technical Details

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.

ECDHE

[View Certificate](#)
[View Cookies](#)
[View Saved Passwords](#)
[Help](#)

1 4 5 7 no IPv6 | 24.3 G1B | DHCP: yes | VPN: no | W: (058% at Tata Decomo Wi-Fi) 100.77.43.199 | E: down | BAT 63.64% | 0.33 | 2017-11-06 14:20:10



Downloads Google - Mozilla Firefox Page Info - https://www.google.co.in/

General Media Permissions **Security**

Website Identity

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

[View Certificate](#)

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**

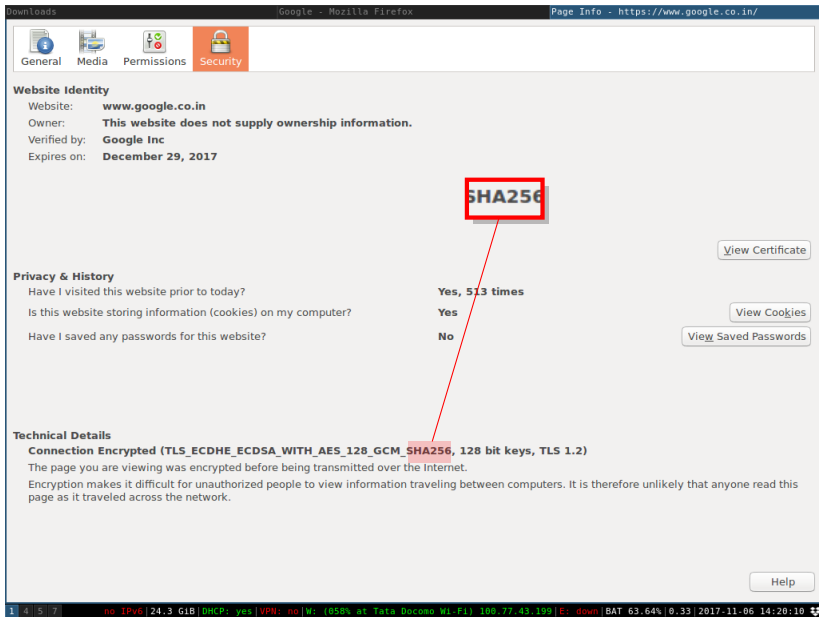
[View Cookies](#)
[View Saved Passwords](#)

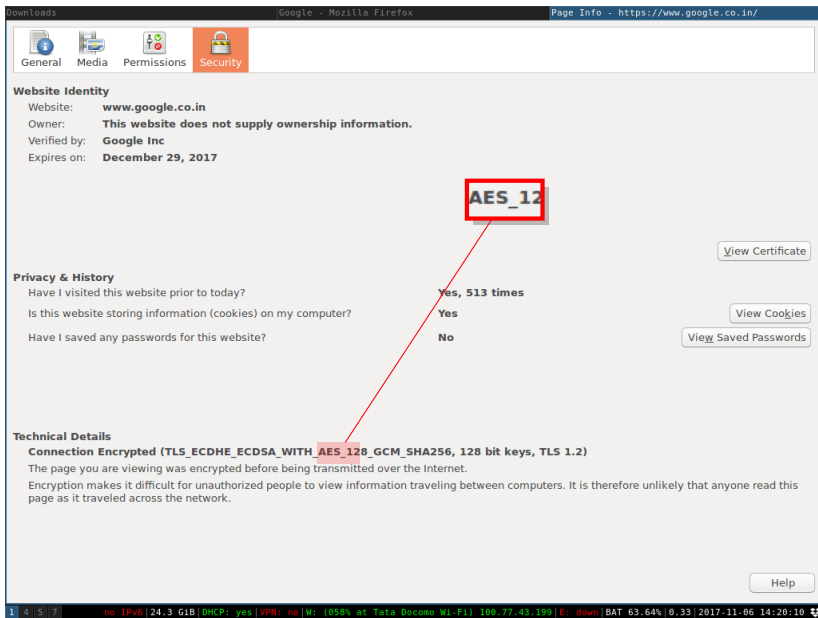
Technical Details

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.

[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

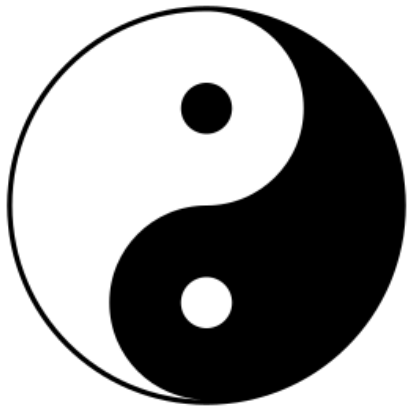




By Dutch cryptographer
Auguste Kerckhoffs

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

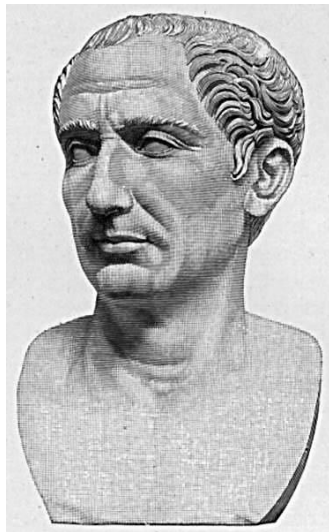
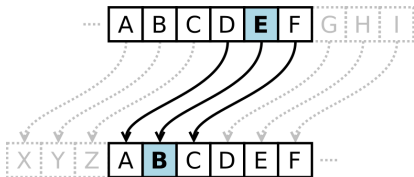
- ▶ ~~Security through obscurity~~
- ▶ However, some parameter must be **secret**
 - ▶ Known only to authorized entities: Alice, Bob
 - ▶ That parameter is the “key”
 - ▶ Distinguishes between Bob and Eve



Yin and Yang

Cryptography & Cryptanalysis

- ▶ 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



- ▶ Applies **modular arithmetic**
- ▶ Letter \leftrightarrow number translation

$$a \rightarrow 0, b \rightarrow 1, c \rightarrow 2, \dots, z \rightarrow 25$$

Encryption

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

Decryption

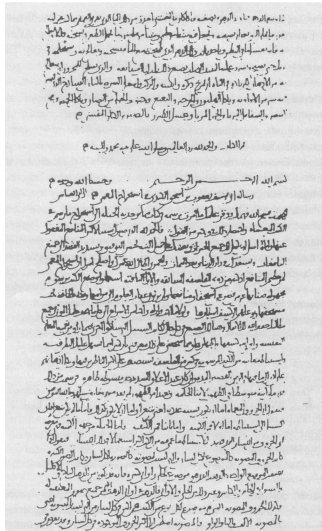
$$d(x) = (x - k) \bmod 26$$

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

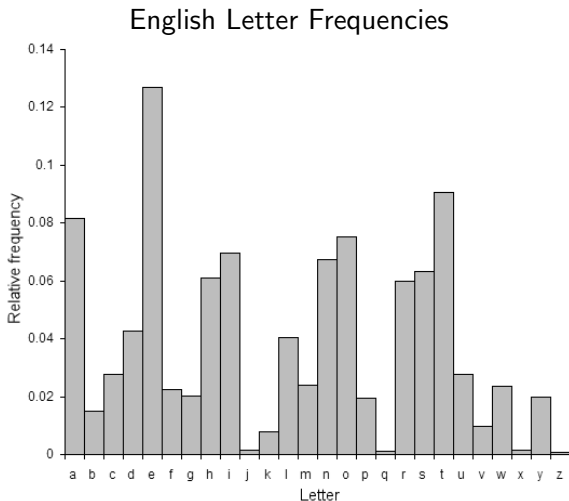
- ▶ Earliest reference on code-breaking
- ▶ 9th Century Arab scientist - **al-Kindi**
- ▶ Rediscovered in 1987 in Istanbul

A Manuscript on Deciphering Encrypted Messages

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



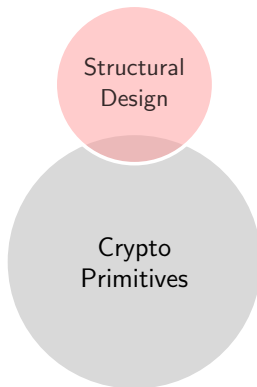
The first page of al-Kindi's manuscript
On Deciphering Cryptographic Messages

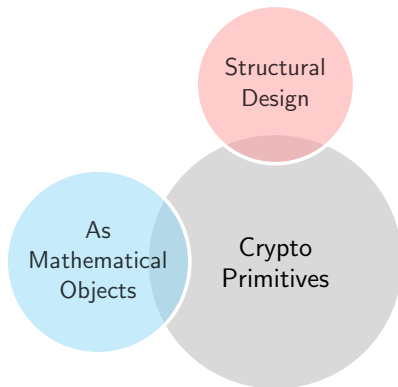


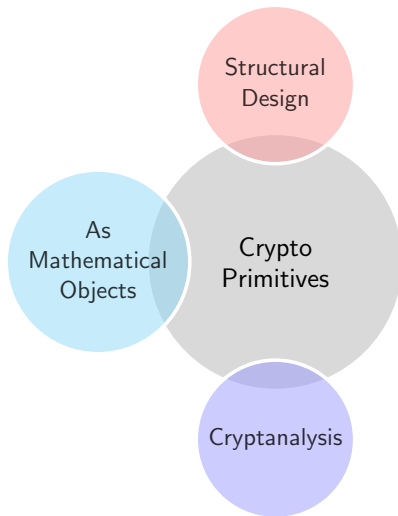
- Can be used to break Caesar Cipher. How?

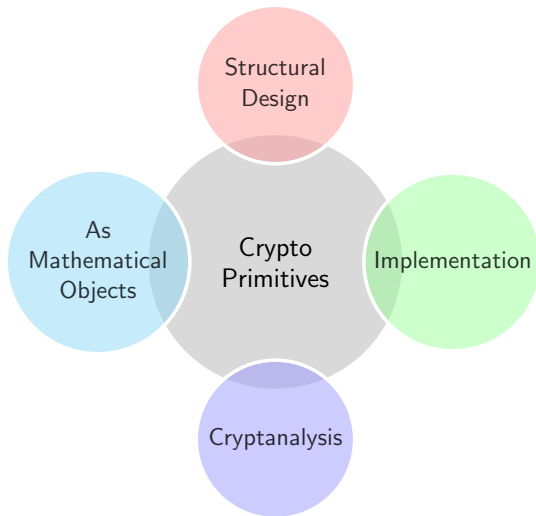


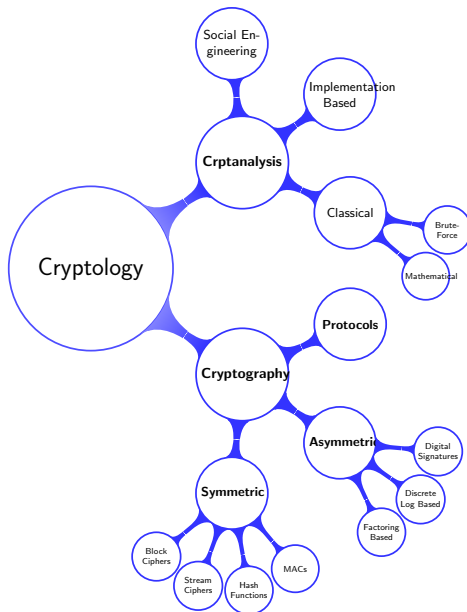
Crypto
Primitives











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.

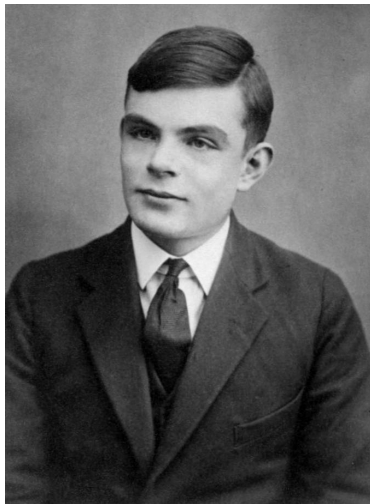
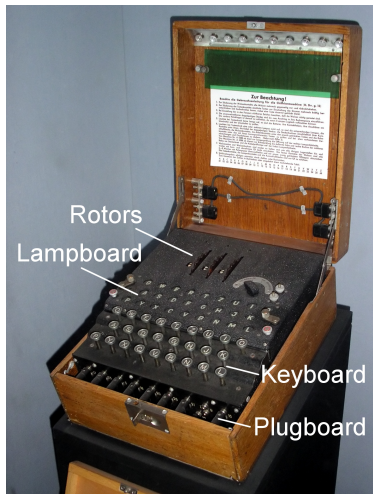
Note

Shift-Cipher and Enigma are already taken.

- ▶ 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!

Hail Crypto!



See you in next class.