Modern Cryptography

Introduction

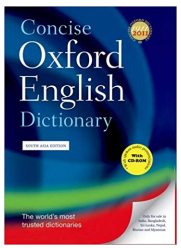
Shashank Singh

IISER Bhopal

August 6, 2025

Cryptography

What is Cryptography?



"the art of writing and solving codes"

for

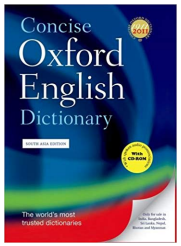
"secret communication"

Do not confuse it with Coding Theory!

- The above definition is historically accurate, but it doesn't capture the scientific foundations of today's "Modern Cryptography".

Cryptography

What is Cryptography?



"the art of writing and solving codes"

for

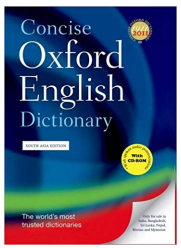
"secret communication"

Do not confuse it with Coding Theory!

- The above definition is historically accurate, but it doesn't capture the scientific foundations of today's "Modern Cryptography".

Cryptography

What is Cryptography?



"the art of writing and solving codes"

for

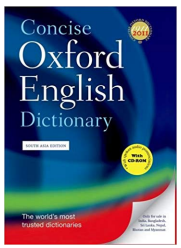
"secret communication"

Do not confuse it with Coding Theory!

- The above definition is historically accurate, but it doesn't capture the scientific foundations of today's "Modern Cryptography".

Cryptography

What is Cryptography?



"the art of writing and solving codes"

for

"secret communication"

Do not confuse it with Coding Theory!

- The above definition is historically accurate, but it doesn't capture the scientific foundations of today's "Modern Cryptography".

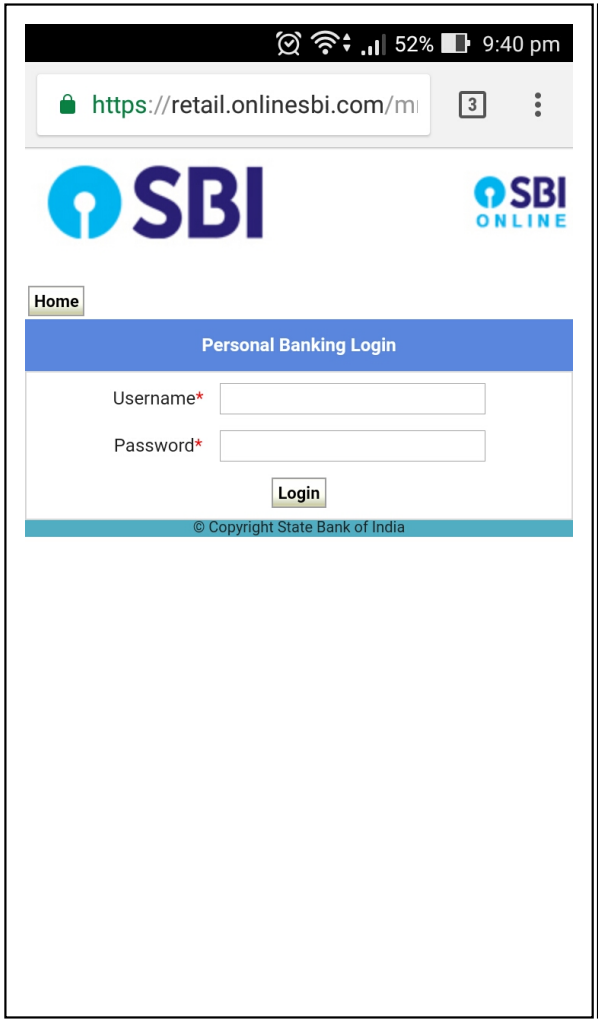
Modern Cryptography

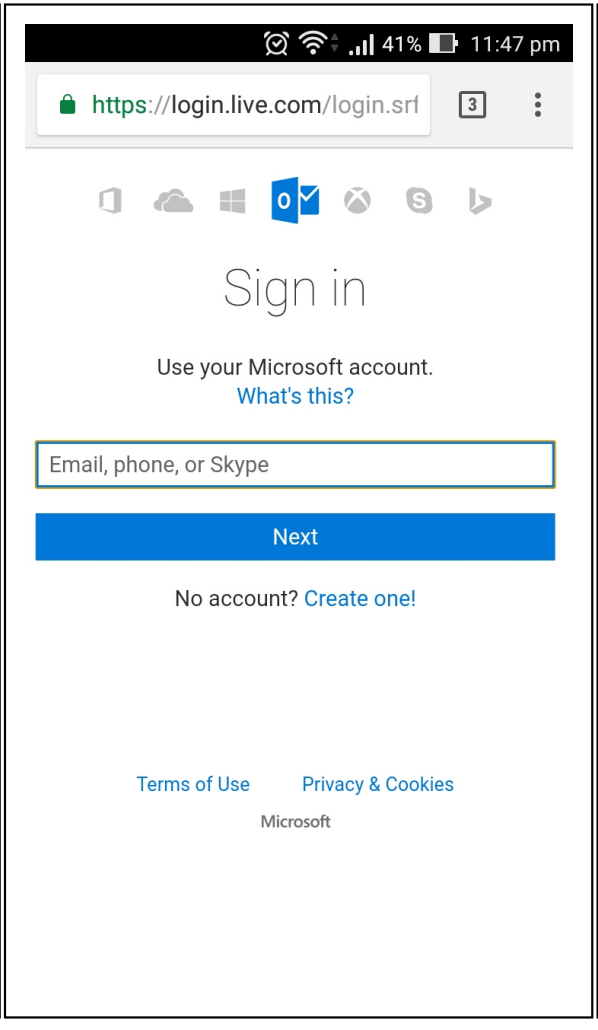
It involves the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks.

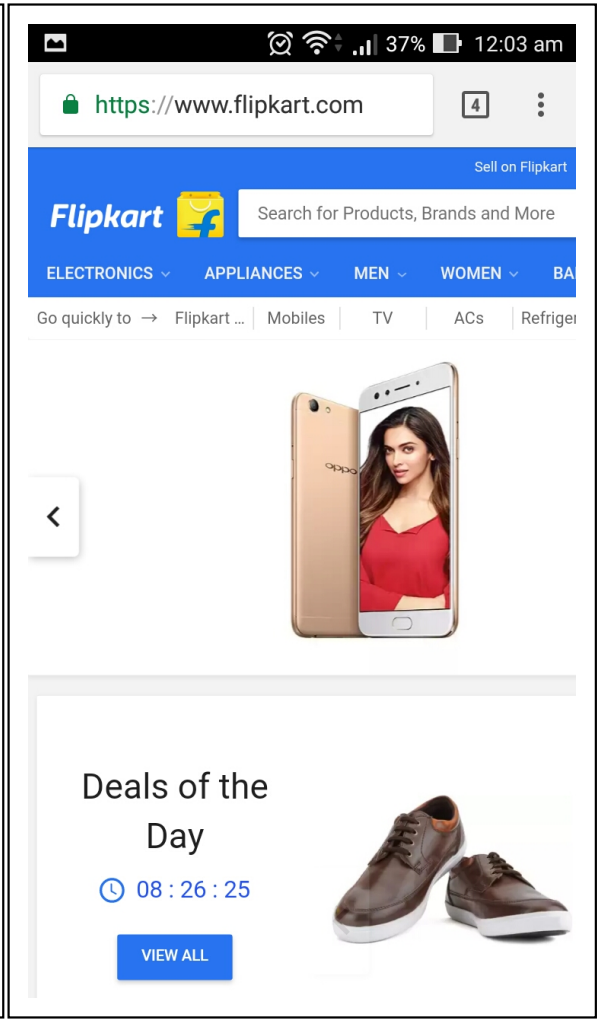
☞ Evolved significantly after the 1970s.

- ✓ Encompasses secret communication and beyond.
- ✓ Recognized as a science and a mathematical discipline.
- ✓ Integrated into our daily lives — we use it almost every day, often without realizing it.

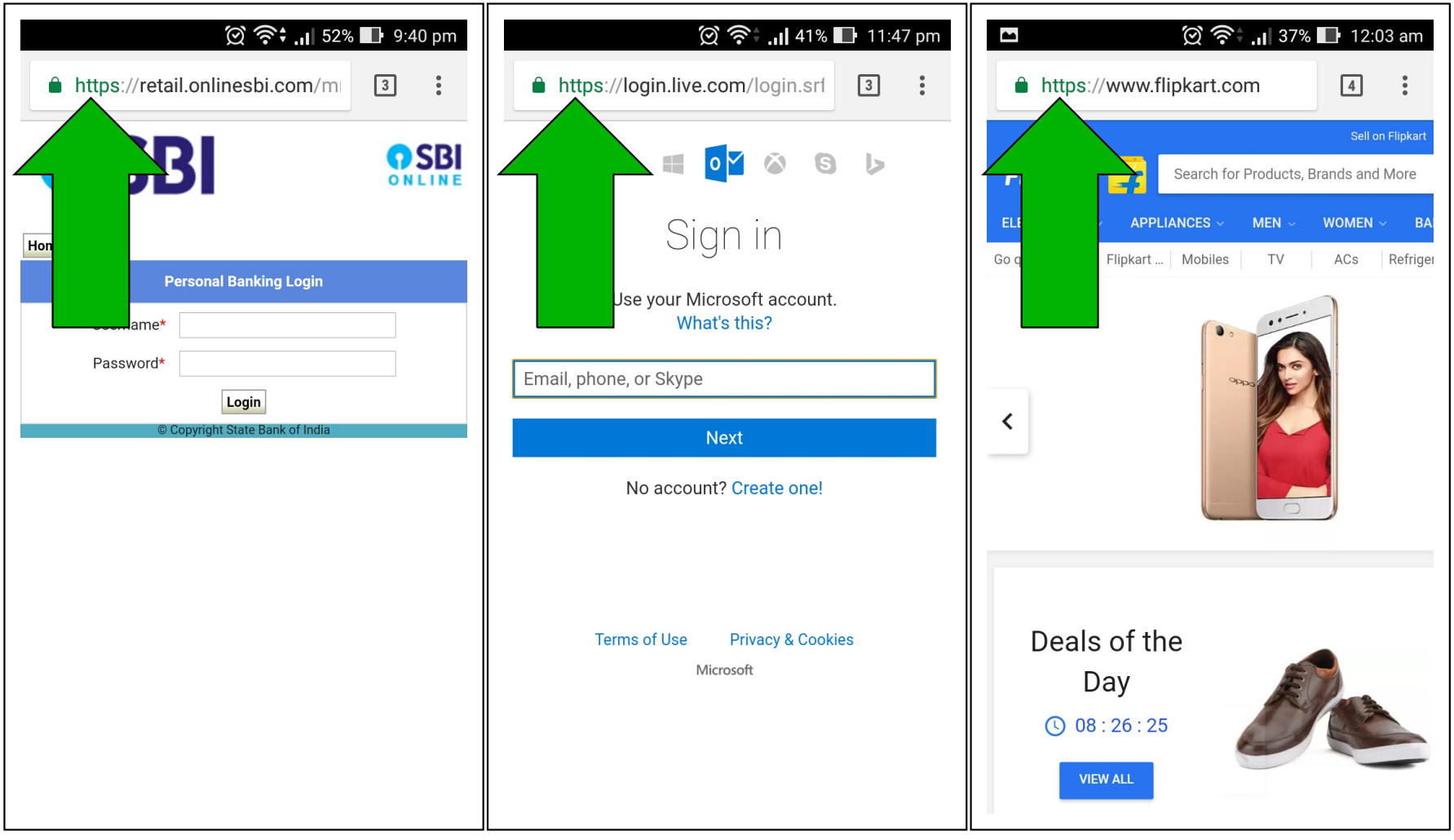
CRYPTOGRAPHY-DO YOU EVER USE IT?



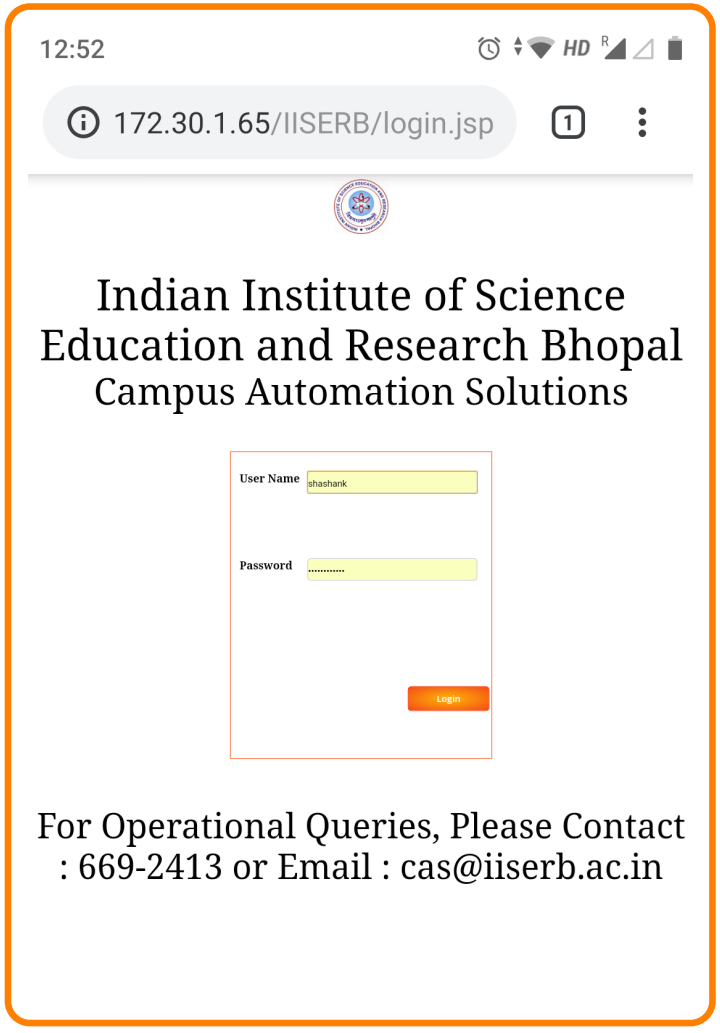




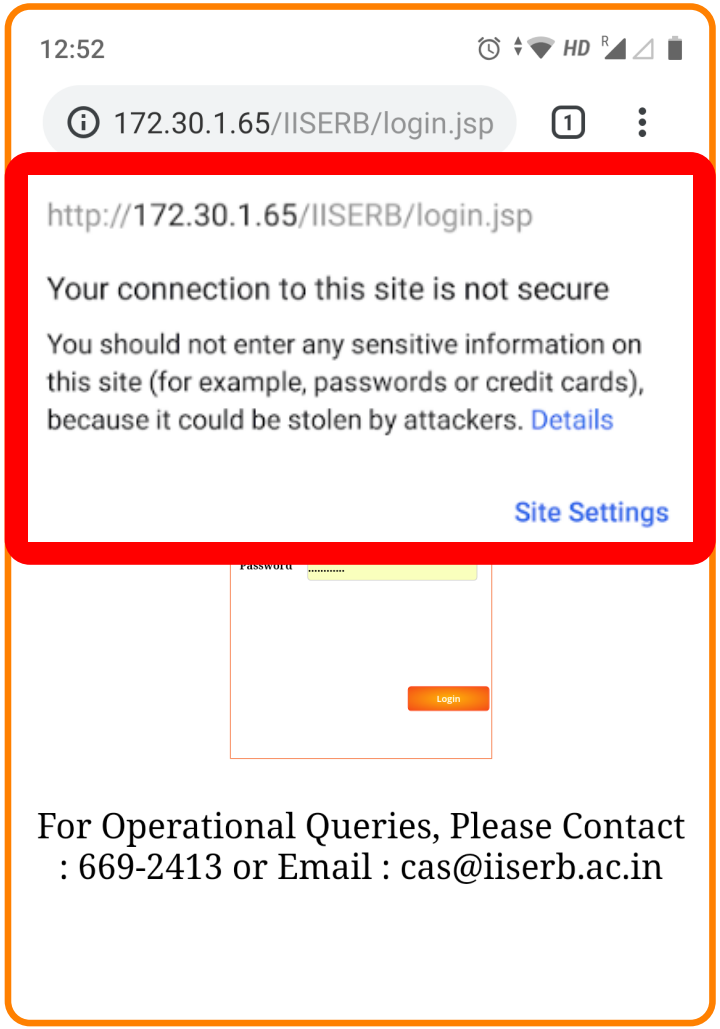
CRYPTOGRAPHY-DO YOU EVER USE IT?



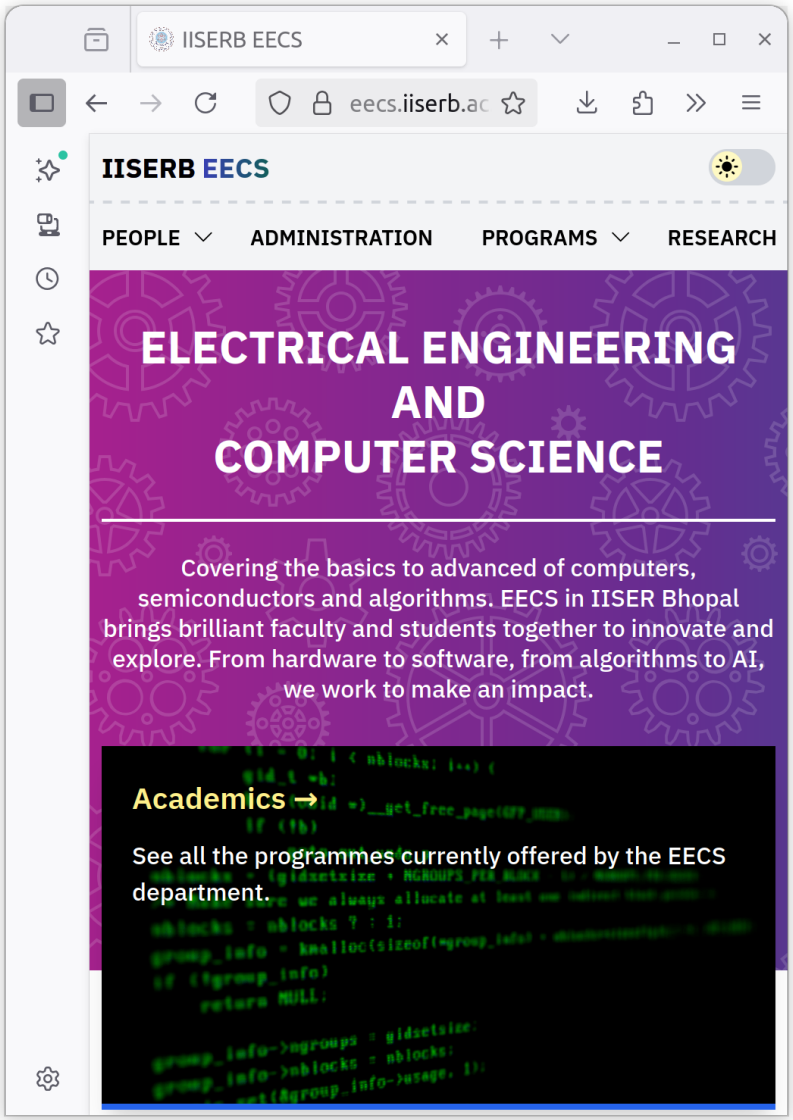
Cryptography-Do you ever use it?..

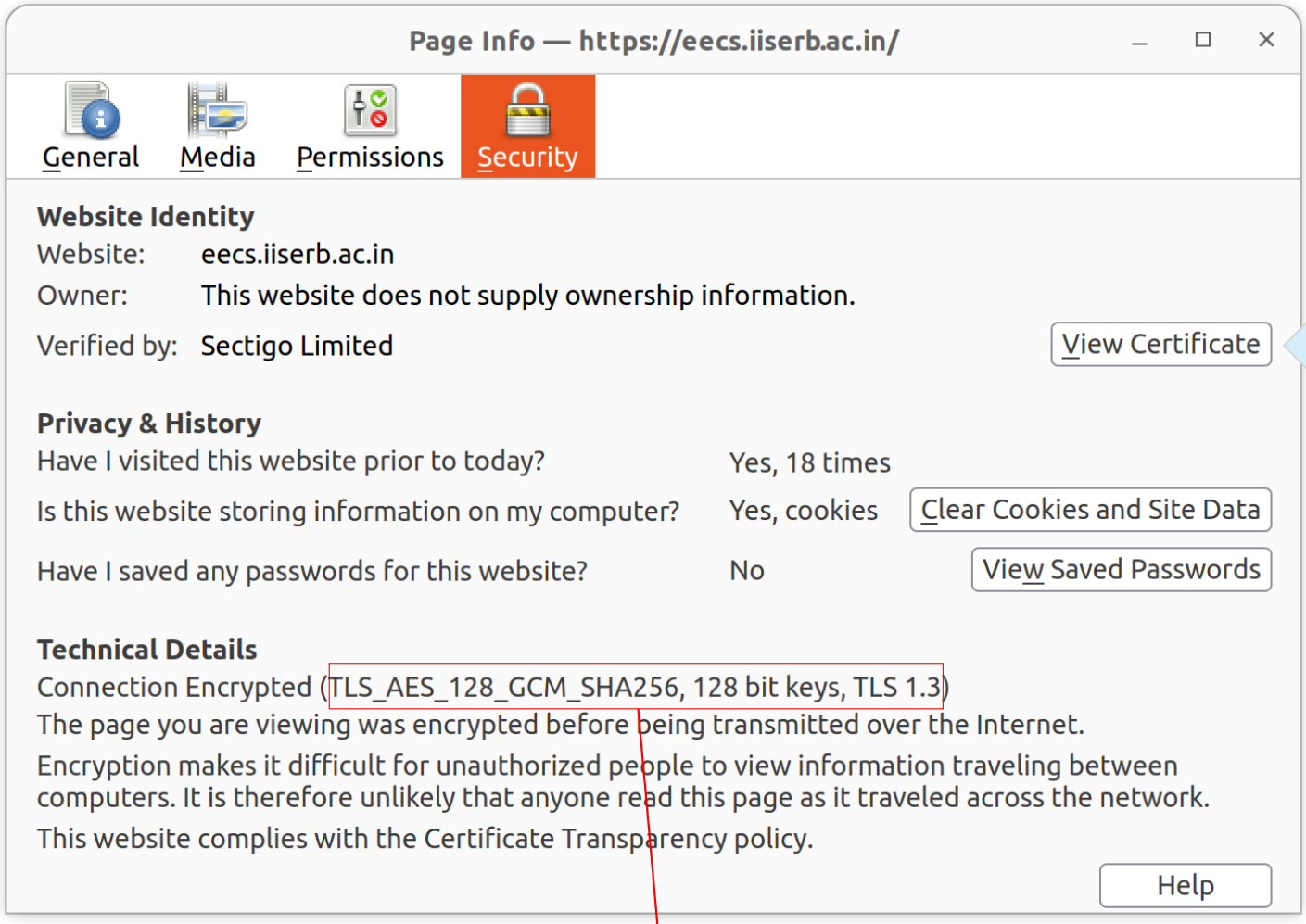


CRYPTOGRAPHY-DO YOU EVER USE IT?..

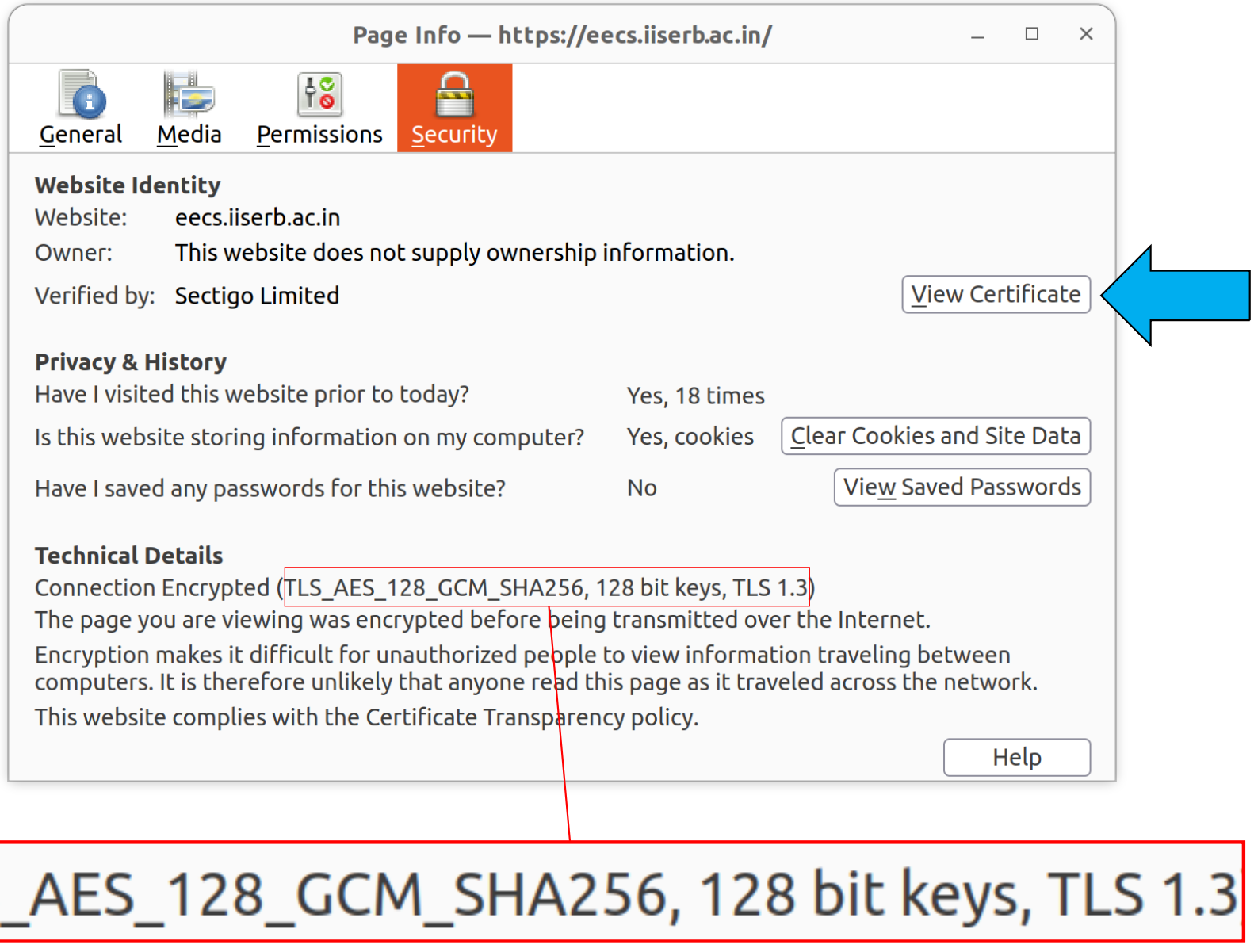


Cryptography in our daily life



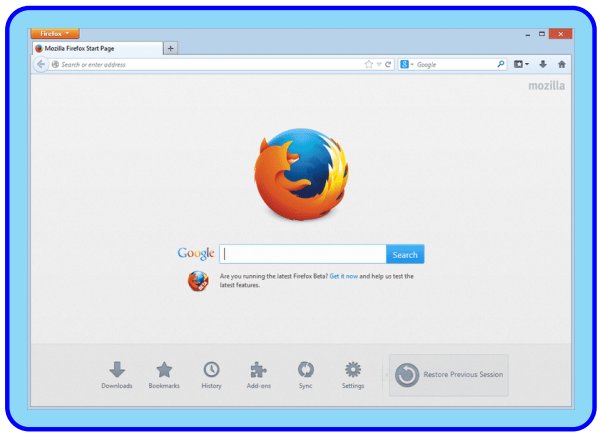


TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3

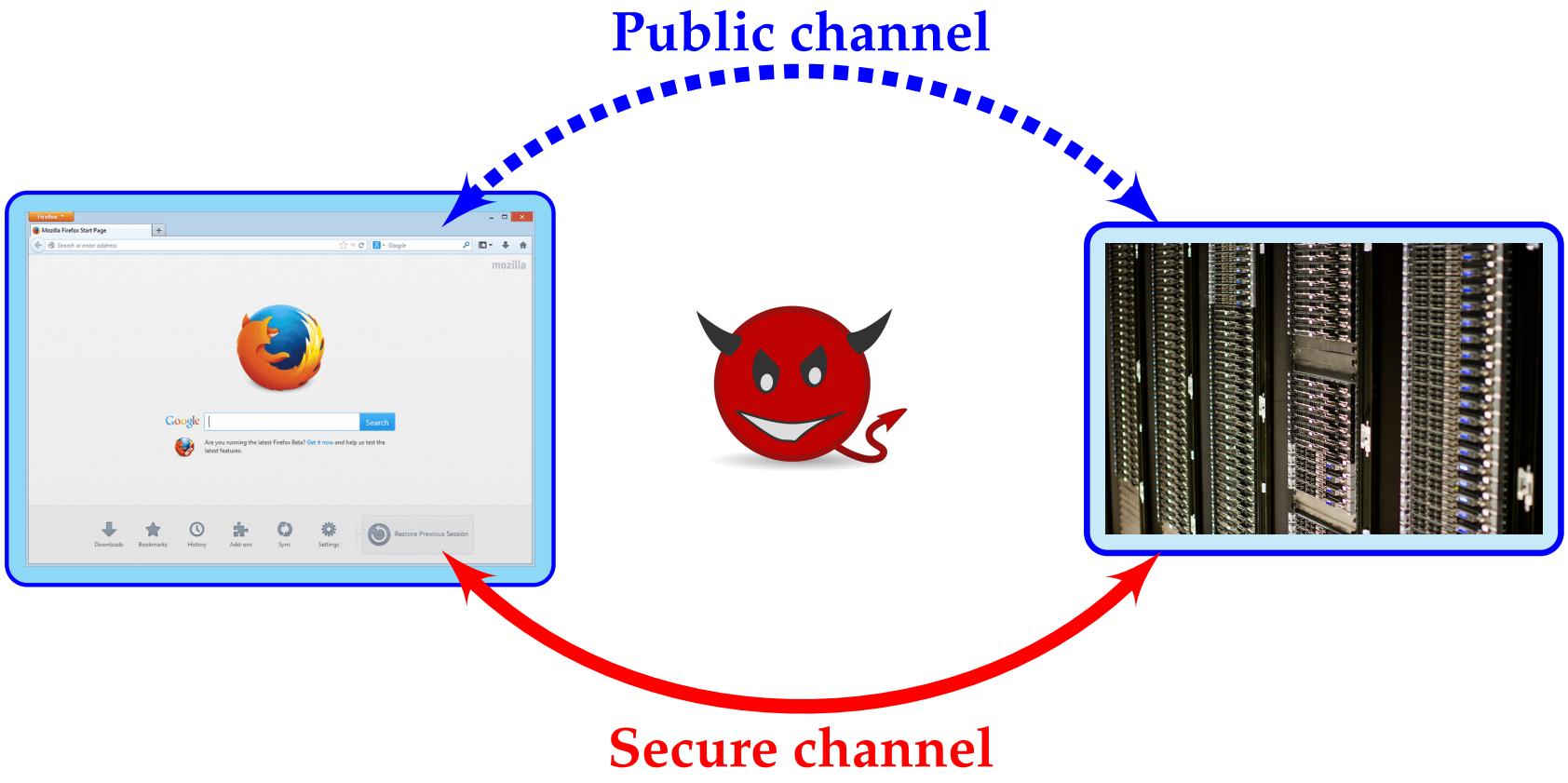

Page Info — https://eecs.iiserb.ac.in/
General
Media
Permissions
Security
Website Identity
Website: eecs.iiserb.ac.in
Owner: This website does not supply ownership information.
Verified by: Sectigo Limited
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 18 times
Is this website storing information on my computer? Yes, cookies
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)
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.
This website complies with the Certificate Transparency policy.
Help
TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3

Secure Communication

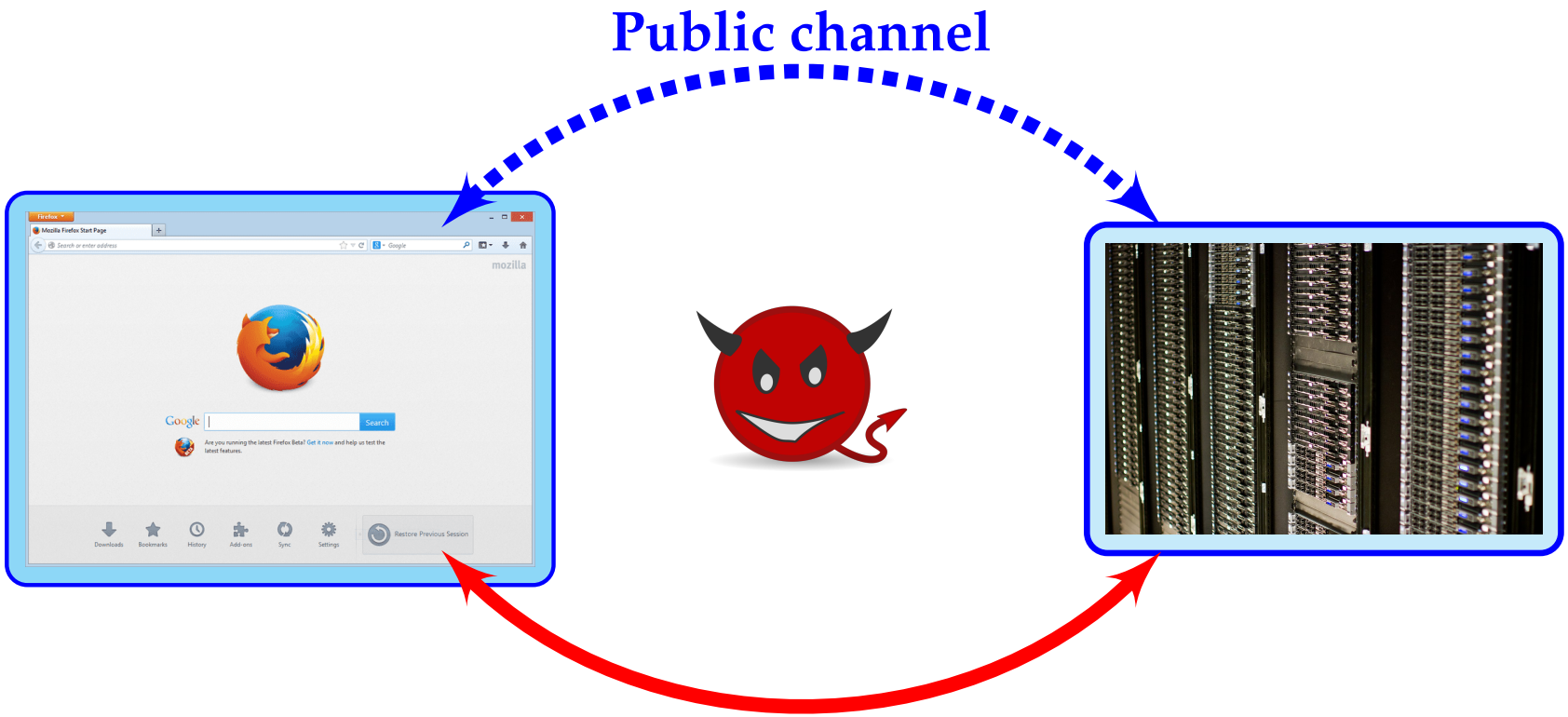
Secure Communication



Secure Communication



Secure Communication

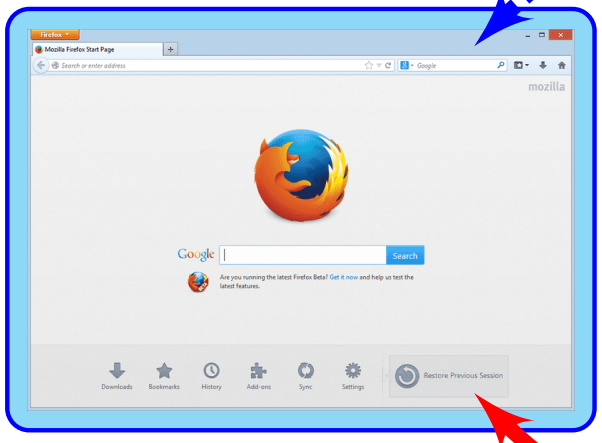


1101010101111111111111001000001110100011100101100011111

Key Exchange/PKC:
How is a secret key shared between the sender and the receiver? Wouldn't this again require a secure channel?

TION

Public channel



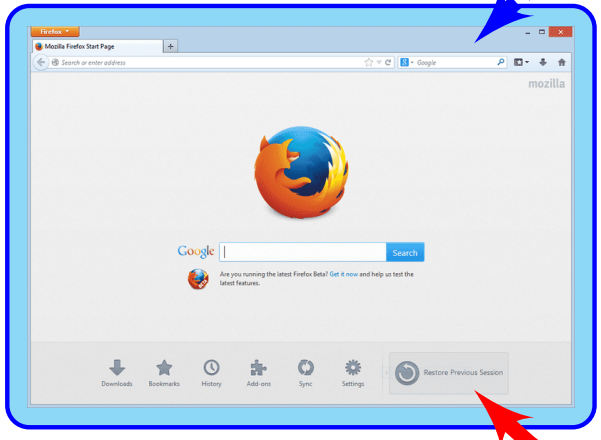
Sec

1101010101111111111111001000001110100011100101100011111

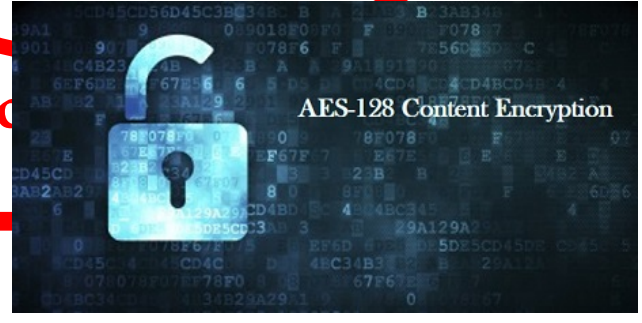
Key Exchange/PKC:
How is a secret key shared between the sender and the receiver? Wouldn't this again require a secure channel?

TION

Public channel



Sec



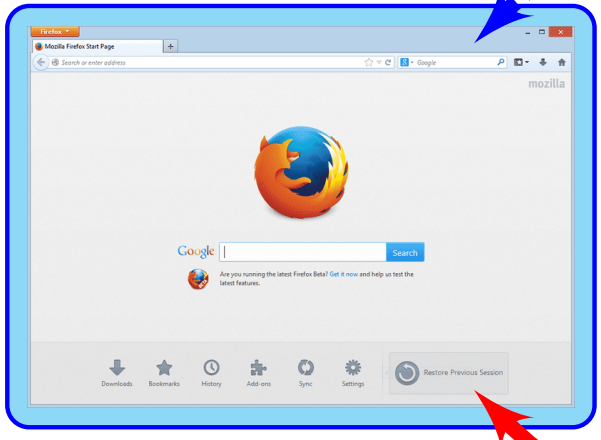
1111111001000001110100011100101100011111

Privacy:
If an adversary eavesdrops the communication, all it gets is a gibberish.

Key Exchange/PKC:
How is a secret key shared between the sender and the receiver? Wouldn't this again require a secure channel?

TION

Public channel



Sec

1111111001000001110 1

Privacy:
If an adversary eavesdrops the communication, all it gets is a gibberish.

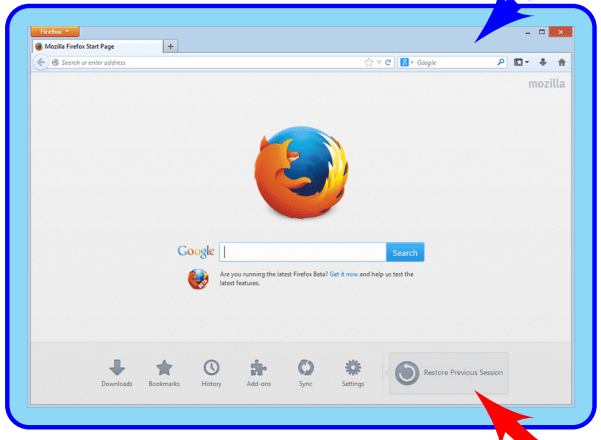
Message Integrity:
What is the guarantee that the message is not modified en-route.

Key Exchange/PKC:
How is a secret key shared between the sender and the receiver? Wouldn't this again require a secure channel?

TION

Public channel

Source Authentication:
How to confirm the sender's identity?
– Digital Certificate
– Digital signature



Sec

1111110010000011101C

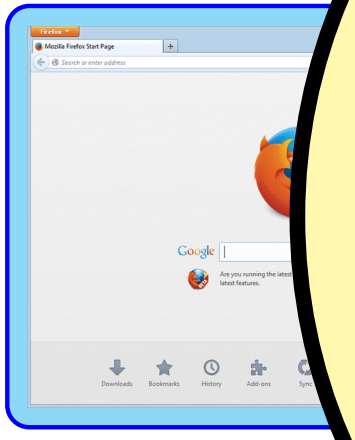
Privacy:
If an adversary eavesdrops the communication, all it gets is a gibberish.

Message Integrity:
What is the guarantee that the message is not modified en-route.

Key Exchange/PKC:
How is a secret key shared between the sender and the receiver? Wouldn't this a
require a secure chann

Source Authentication:
How to confirm the
sender's identity?
igital Certificate
al signature

A very basic aim of Modern Cryptography



Privacy:
If an adversary eaves-drops the communication, all it gets is a gibberish.

ssage Integrity:
What is the guarantee that the message is not modified en-route.

Course Content

- Basic Understanding of Cryptography (Secret Key Cryptography)
- Secret Key Cryptography
  - Introduction, Some Simple Cryptosystems and their Cryptanalysis. (Caesar Cipher, Vigenere Cipher, Substitution-Permutation Cipher etc.)
  - One Time Pad (OTP), Perfect Secrecy (Shannon's Theory) and other Security Notions.
  - Block Ciphers and their analysis.
  - Modes of Operations, Stream Ciphers.
  - Hash Function and their Applications in Cryptography.
  - Authentication and Authentication Encryption.
- Public Key Cryptography
  - Key Exchange Protocols, PKCs (RSA, ElGamal).
  - Computationally Hard Mathematical Problems and the State-of-the-art Algorithm for solving them.
  - Lattice-based cryptography
  - Digital Signatures and ldentification Schemes
  - Security Notions in Public Key Setting.-PKI(Https), TLS, Secret Sharing, Broadcast Encryption, Fingerprinting etc.
- Some other advance cryptographic primitives (basic notions only)

Course Content

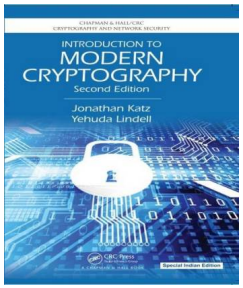
- Basic Und… …ecret Key Cryptography)
- Secret Ke…
  - Introd… …their Cryptanalysis. (Caesar Cipher, Vigene… …her etc.)
  - One Ti… …s Theory) and other Security Notions.
  - Block …
  - Modes of Operations, Stream Ciphers.
  - Hash Function and their Applications in Cryptography.
  - Authentication and Authentication Encryption.
- Public Key Cryptogra…
  - Key Exchange Protoco…
  - Computationally Har… …of-the-art Algorithm for solving them.
  - Lattice-based cryptog…
  - Digital Signatures an… …
  - Security Notions in Pu… …Sharing, Broadcast Encryption, Fingerpri…ting etc.
- Some other advance cryptographic primitives (basic notions only)

Weightage

- Midesemester 30%
- Endsemester 50%
- Quiz/Assignment 20%

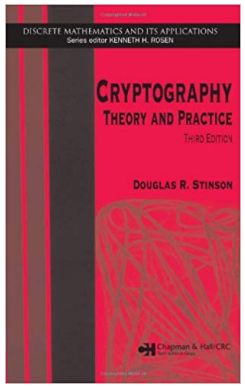
The deadline for quiz/assignment will be strict. No request for extension will be entertained.

Books



Introduction to Modern Cryptography, 2nd Ed. (Book by Jonathan Katz and Yehuda Lindell)

Cryptography: Theory and Practice, Third Edition (Book by Douglas R. Stinson)



Setting of Private-key Cryptography..

Classical Cryptography

- Before sending the message (plaintext) m, Alice transforms (encrypts) it into a message c (ciphertext), using an algorithm ENC and a key k.
- Bob, on receiving c, decrypts it to get m, using a corresponding algorithm DEC and the same key k.

Setting of Private-key Cryptography..

Classical Cryptography

- The key k, needs to be (somehow) shared between the two communicating parties in advance and it is not known to the adversary.
- Alice and Bob could be same. Recall the disk encryption, where the same party encrypts the data on a disk and later decrypts it to get back the data.