Introduction to Cryptography

Dhananjoy Dey

Indian Institute of Information Technology, Lucknow
ddey@iiitl.ac.in

January 18, 2021

Disclaimers

All the pictures used in this presentation are taken from freely available websites.

Disclaimers

All the pictures used in this presentation are taken from freely available websites.

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

Disclaimers

All the pictures used in this presentation are taken from freely available websites.

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement nor does it imply that the products mentioned are necessarily the best available for the purpose.

Outline

1. Introduction
   - What is Cryptography?
   - Syllabus
   - References
   - Why do we require Cryptography?

Outline

Cryptology

Cryptology

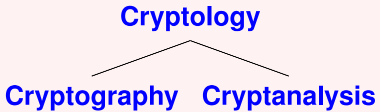
Cryptology

Cryptology

Cryptography **Cryptanalysis**

Cryptology

Cryptology



Cryptology

- **Cryptography:** is a science which deals with how to achieve '**PAIN**'

Cryptology

Cryptology

Cryptology

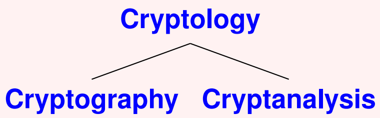
Cryptography **Cryptanalysis**

Cryptology

- **Cryptography:** is a science which deals with how to achieve '**PAIN**'
  '**P**rivacy',(Confidentiality)
  Authentication,
  Integrity &
  Non-repudiation.

Cryptology

Cryptology



Cryptology

- **Cryptography:** is a science which deals with how to achieve '**PAIN**'
  '**P**rivacy',(Confidentiality)
  Authentication,
  Integrity &
  Non-repudiation.
- **Cryptanalysis:** is a science which deals with how to defeat of achieving '**PAIN**'

Cryptology

Cryptology

Cryptology

Cryptography **Cryptanalysis**

Cryptology

- **Cryptography:** is a science which deals with how to achieve '**PAIN**'
  '**P**rivacy',(Confidentiality)
  Authentication,
  Integrity &
  Non-repudiation.
- **Cryptanalysis:** is a science which deals with how to defeat of achieving '**PAIN**'

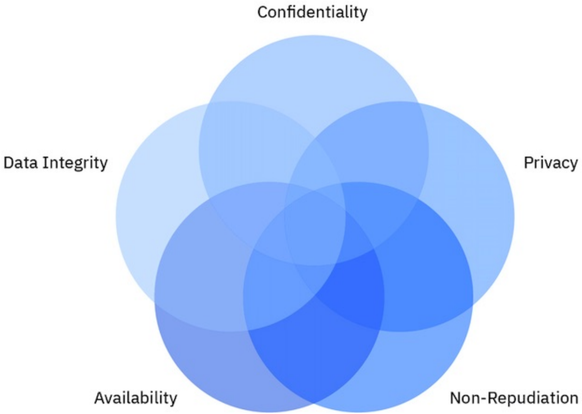
Cryptography is about communication in the presence of an adversary.

— Rivest

विद्या ददाति विनयं विनयाद् याति पात्रताम्

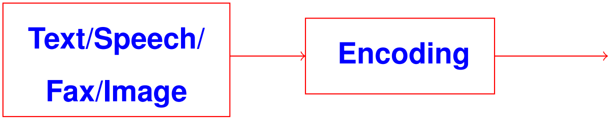
Cryptography

Cryptography supports multiple goals

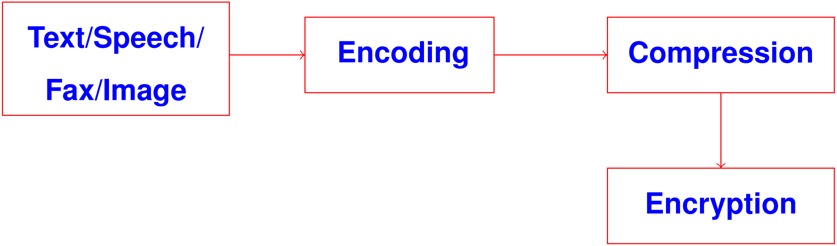


Cryptography for Secure Communication

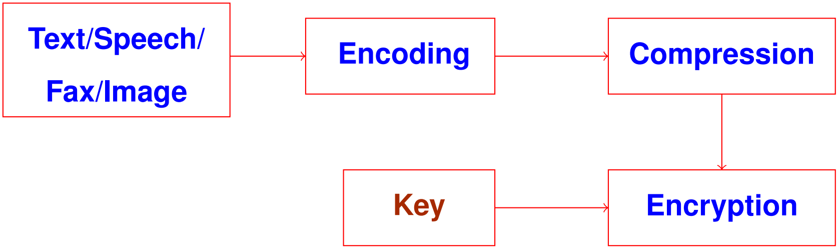
Cryptography for Secure Communication



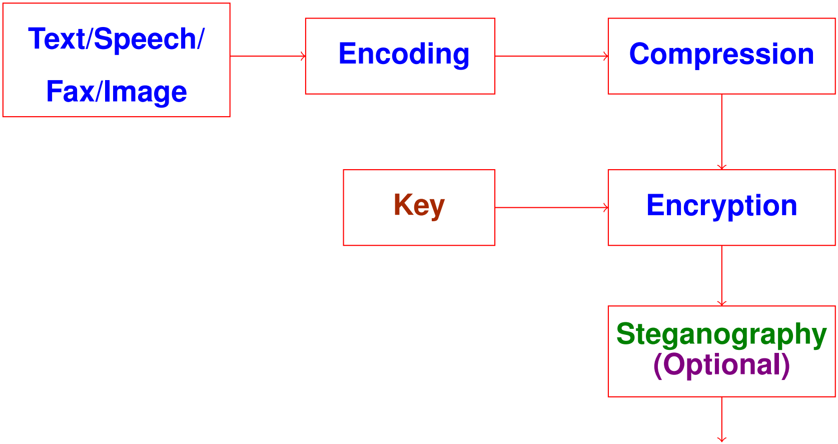
Cryptography for Secure Communication



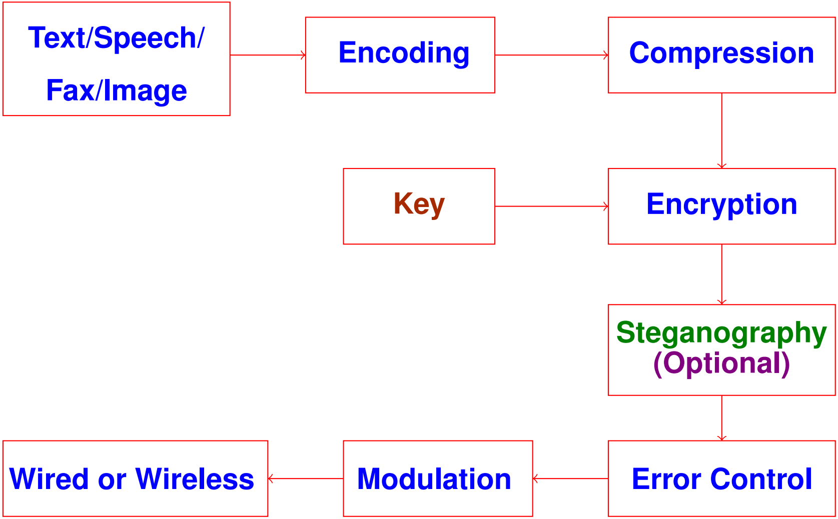
Cryptography for Secure Communication



Cryptography for Secure Communication



Cryptography for Secure Communication



Course Contents – Cryptography

- **Introduction to Cryptography**
- **Private-Key Cryptography**
  - Classical Cryptography
  - Shannon's Theory, Perfect Secrecy, and the One-Time Pad
  - Block Ciphers
  - Stream Ciphers
  - Message Authentication
- **Key-less Cryptography**
  - Random Number Generators
  - Hash Functions
- **Public-Key Cryptography**
  - Diffie-Hellman Key Exchange
  - The RSA Cryptosystem
  - The ElGamal Cryptosystem
  - Elliptic Curves Cryptosystem
  - Digital Signature Schemes

Course Contents – Network Security I

- **Transport-Level Security**
  - Web Security Considerations
  - Transport Layer Security
  - HTTPS
  - SSH
- **Wireless Network Security**
  - Wireless Security
  - Mobile Device Security
  - IEEE 802.11 & IEEE 80.11i
- **Email Security**
  - Internet Mail Architecture
  - Email Threat and Comprehensive Email Security
  - S/MIME
  - DNS-based Authentication
  - Sender Policy Framework

Course Contents – Network Security II

- Domain-keys Identified Mail
- Domain-based Message Authentication

- **IP Security**
  - IP Security Policy
  - Encapsulating Security Payload
  - Internet Key Exchange
- **Network Endpoint Security**
  - Firewalls
  - Intrusion Detection System
  - Malicious Software
  - Distributed Denial of Service Attacks
- **Cloud Security**
- **Security**

References

- **Textbook**

D. R. Stinson & M. B. Paterson,
Cryptography – Theory and Practice, CRC, 2019.

William Stallings,
Cryptography and Network Security: Principles and Practice, Pearson Education Canada, 2020.

References

- **Supplementary Reading**

J. Katz & Y. Lindell,
Introduction to Modern Cryptography, CRC Press, 2015.

Neal Koblitz,
A Course in Number Theory and Cryptography, Springer- Verlag, 1994.

Keith Martin,
Cryptography: The Key to Digital Security, How It Works, and Why It Matters, W. W. Norton & Company, 2020.

Nigel P. Smart,
Cryptography Made Simple, Springer, 2016.

Mark Stamp,
Information Security: Principles and Practice, John Wiley & Sons, 2011.

Components of Cryptosystems

Components of Cryptosystems

- **Plaintext-space:** P – a set of plaintexts over an alphabet $\sum$
- **Ciphertext-space:** C – a set of ciphertexts over alphabet Δ
- **Key-space:** K – a set of keys

Components of Cryptosystems

- **Plaintext-space:** P – a set of plaintexts over an alphabet $\sum$
- **Ciphertext-space:** C – a set of ciphertexts over alphabet Δ
- **Key-space:** K – a set of keys

  Each key k determines an encryption algorithm e_k and an decryption algorithm d_k such that, for any plaintext w, $e_k(w)$ is the corresponding ciphertext and

$$w = d_k(e_k(w)).$$

Requirements for Good Cryptosystems

Requirements for Good Cryptosystems

- Given e_k and a plaintext w, it should be easy to compute $c = e_k(w)$.
- Given d_k and a ciphertext c, it should be easy to compute $w = d_k(c)$.

Requirements for Good Cryptosystems

- Given e_k and a plaintext w, it should be easy to compute $c = e_k(w)$.
- Given d_k and a ciphertext c, it should be easy to compute $w = d_k(c)$.
- A ciphertext $e_k(w)$ should not be much longer than the plaintext w.

Requirements for Good Cryptosystems

- Given e_k and a plaintext w, it should be easy to compute $c = e_k(w)$.
- Given d_k and a ciphertext c, it should be easy to compute $w = d_k(c)$.
- A ciphertext $e_k(w)$ should not be much longer than the plaintext w.
- It should be infeasible to determine w from $e_k(w)$ without knowing d_k.

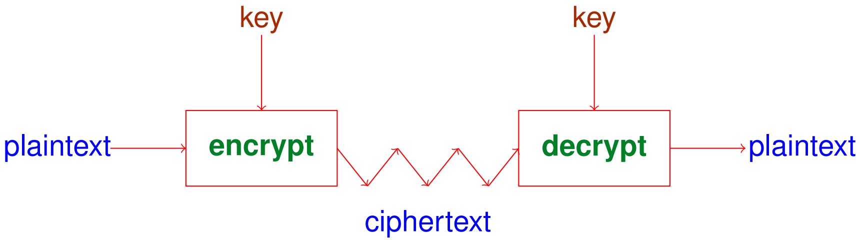
Requirements for Good Cryptosystems

- Given e_k and a plaintext w, it should be easy to compute $c = e_k(w)$.
- Given d_k and a ciphertext c, it should be easy to compute $w = d_k(c)$.
- A ciphertext $e_k(w)$ should not be much longer than the plaintext w.
- It should be infeasible to determine w from $e_k(w)$ without knowing d_k.
- The so called avalanche effect should hold.

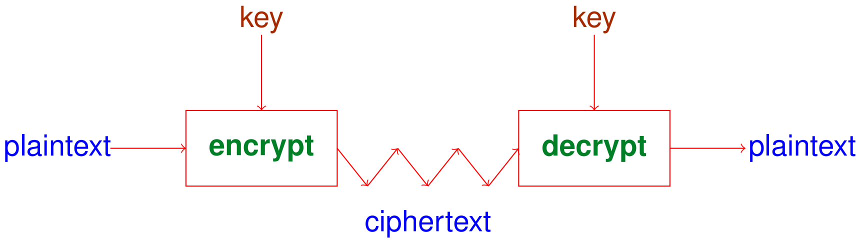
Requirements for Good Cryptosystems

- Given e_k and a plaintext w, it should be easy to compute $c = e_k(w)$.
- Given d_k and a ciphertext c, it should be easy to compute $w = d_k(c)$.
- A ciphertext $e_k(w)$ should not be much longer than the plaintext w.
- It should be infeasible to determine w from $e_k(w)$ without knowing d_k.
- The so called avalanche effect should hold.
- The cryptosystem should not be closed under composition, i.e. not for every two keys k_1, k_2 $\exists$ a key k s/t $e_k(w) = e_{k_1}(e_{k_2}(w))$.
- The set of keys should be very large.

A Generic View of Secret Key Crypto

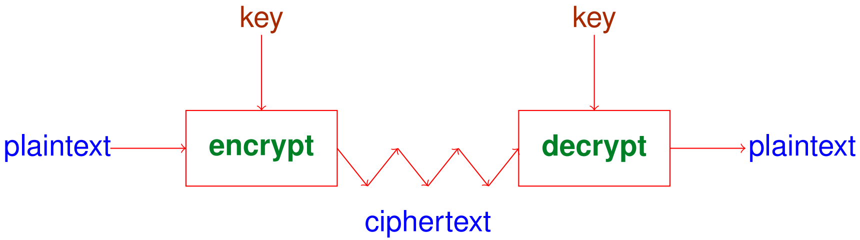


A Generic View of Secret Key Crypto



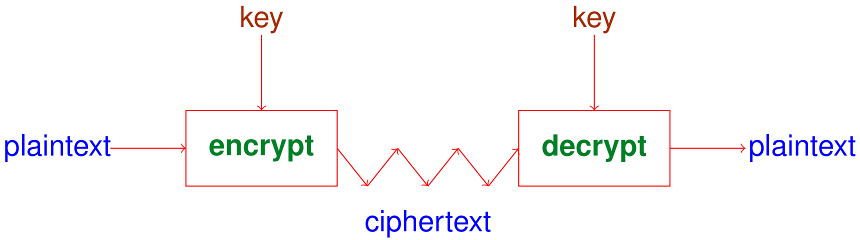
- Sender and receiver use the same key
- Sender and receiver are equivalent
- The oldest type of cryptography
- Gives the best performance
- Provides highest security standards

A Generic View of Secret Key Crypto



- Sender and receiver use the same key
- Sender and receiver are equivalent
- The oldest type of cryptography
- Gives the best performance
- Provides highest security standards
- Only disadvantage:

A Generic View of Secret Key Crypto



- Sender and receiver use the same key
- Sender and receiver are equivalent
- The oldest type of cryptography
- Gives the best performance
- Provides highest security standards
- Only disadvantage: difficult key management

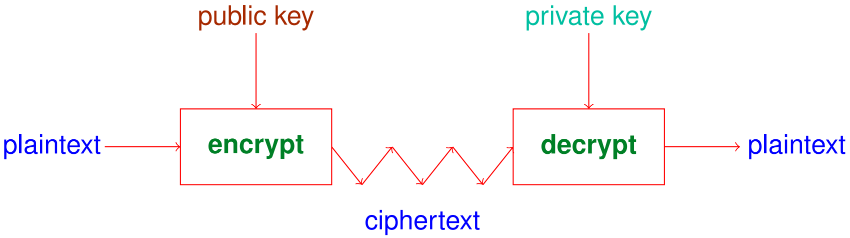
Secret Key Crypto

Classification

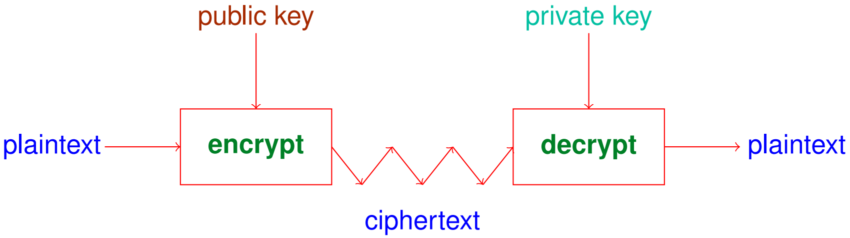
Secret Key Cryptography

- Block
- Stream
- MAC

A Generic View of Public Key Crypto



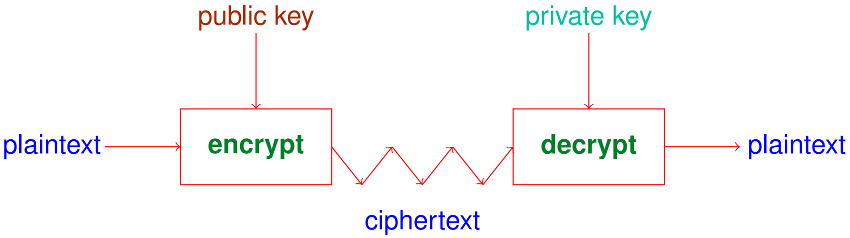
A Generic View of Public Key Crypto



Advantages over symmetric-key

1. Better key distribution and management
   - No danger that public key compromised
2. New protocols
   - Digital Signature
3. Long-term encryption

A Generic View of Public Key Crypto

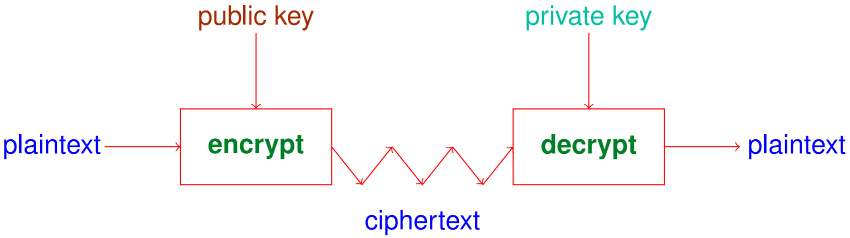


Advantages over symmetric-key

1. Better key distribution and management
   - No danger that public key compromised
2. New protocols
   - Digital Signature
3. Long-term encryption

Only disadvantage:

A Generic View of Public Key Crypto



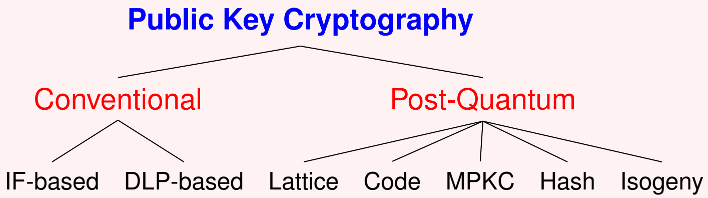
Advantages over symmetric-key

1. Better key distribution and management
   - No danger that public key compromised
2. New protocols
   - Digital Signature
3. Long-term encryption

Only disadvantage: much more slower than symmetric key crypto

Public Key Crypto

Classification



Principle

The philosophy of modern cryptanalysis is embodied in the following principle formulated in 1883

- Basic assumptions:
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms are not secret

Principle

The philosophy of modern cryptanalysis is embodied in the following principle formulated in 1883

- Basic assumptions:
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms are not secret
- This is known as *Kerckhoffs' Principle*

Principle

The philosophy of modern cryptanalysis is embodied in the following principle formulated in 1883

- Basic assumptions:
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms are not secret
- This is known as *Kerckhoffs' Principle*

- Why do we make this assumption?

Principle

The philosophy of modern cryptanalysis is embodied in the following principle formulated in 1883

- Basic assumptions:
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms are not secret
- This is known as *Kerckhoffs' Principle*

- Why do we make this assumption?
  - Easier to maintain secrecy of a short key rather than an algorithm

Principle

The philosophy of modern cryptanalysis is embodied in the following principle formulated in 1883

- Basic assumptions:
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms are not secret
- This is known as *Kerckhoffs' Principle*

- Why do we make this assumption?
  - Easier to maintain secrecy of a short key rather than an algorithm
    - Algorithm parts may be leaked: insider or reverse engineering.

Principle

The philosophy of modern cryptanalysis is embodied in the following principle formulated in 1883

- Basic assumptions:
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms are not secret
- This is known as *Kerckhoffs' Principle*

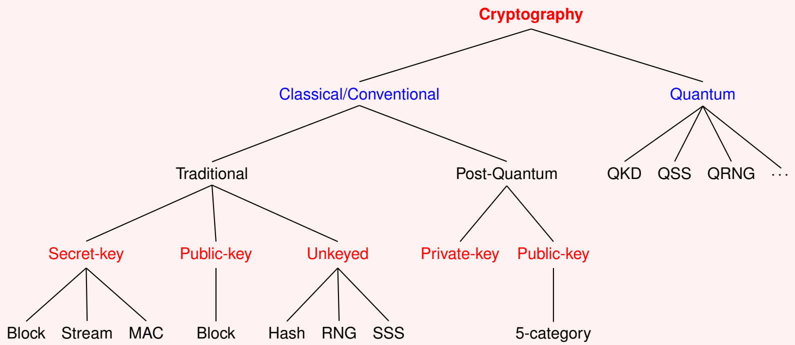
- Why do we make this assumption?
  - Easier to maintain secrecy of a short key rather than an algorithm
    - Algorithm parts may be leaked: insider or reverse engineering.
  - Key revocation/reissue is easier than algorithm revocation/reissue
  - Different people communication: different keys or different algorithms?

विद्या ददाति विनयं विनयाद् याति पात्रताम्

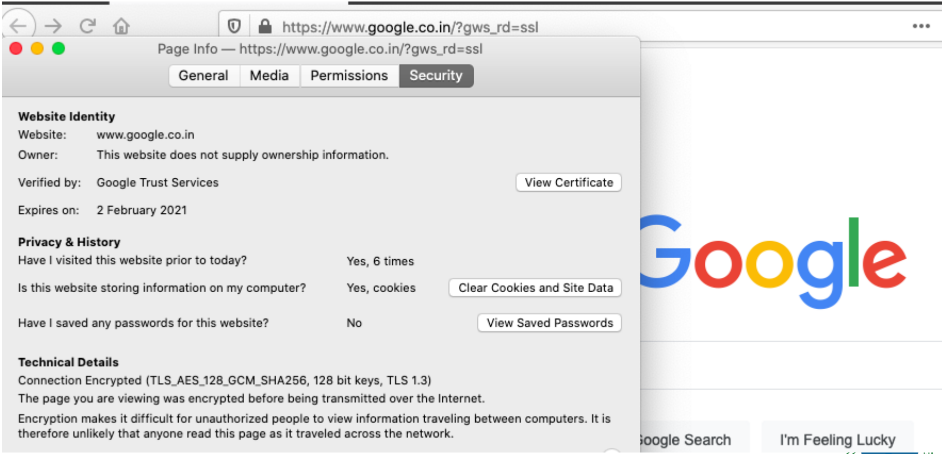
Classification of Cryptography

Classification of Cryptography

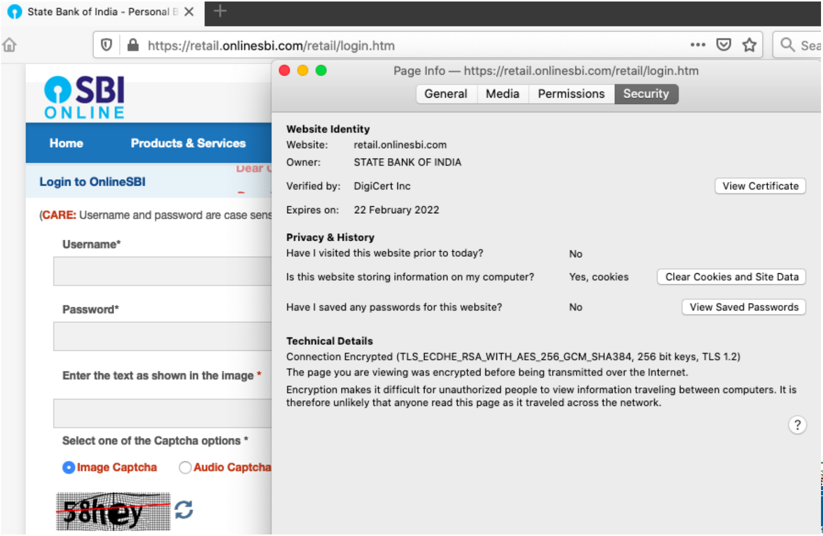
Classification



Cryptography is Everywhere



Cryptography is Everywhere



Cryptography is Everywhere

Figure: e-KYC Service Provided by the UIDAI

Cryptography is Everywhere

Figure: e-KYC Service Provided by the UIDAI

- $SHA\text{-}256(the\ KYC\ data)$ is computed and attached.

Cryptography is Everywhere

Figure: e-KYC Service Provided by the UIDAI

- $SHA\text{-}256(the\ KYC\ data)$ is computed and attached.
- *KYC data* along with *the computed hash* are encrypted using AES-256.

Cryptography is Everywhere

Figure: e-KYC Service Provided by the UIDAI

- $SHA\text{-}256(\mathit{the\ KYC\ data})$ is computed and attached.
- *KYC data* along with *the computed hash* are encrypted using AES-256.
- The *encrypted data* and *hash* are digitally signed by UIDAI using RSA-2048.

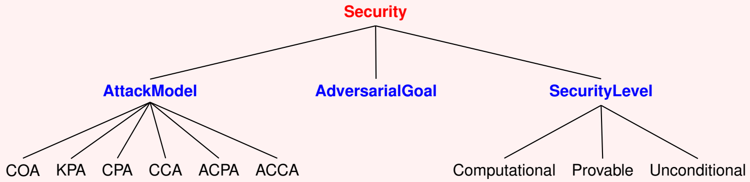
Cryptography is Everywhere

- ATM machines
- All HTTPS websites
- Remote login and file transfer (SSH, . . .)
- Mobile communication (GSM, . . .)
- Wireless networking (Wi-Fi, WiMAX, . . .)
- . . .

Security in Cryptography

Security in Cryptography

Security Classification

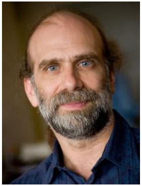


“Encryption works. Properly implemented strong cryptosystems are one of the few things that you can rely on."

- - Edward Snowden

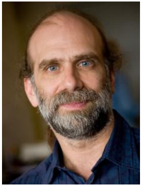
“Encryption works. Properly implemented strong cryptosystems are one of the few things that you can rely on."

- - Edward Snowden



“Encryption works. Properly implemented strong cryptosystems are one of the few things that you can rely on."

- - Edward Snowden



“Trust the math. Encryption is your friend. Use it well and do your best to ensure that nothing can compromise it. That’s how you can remain secure even in the face of the NSA."

- - Bruce Schneier

While cryptography is important, it must be clear that it is not a magic wand that solves all the security problems in IT systems.

While cryptography is important, it must be clear that it is not a magic wand that solves all the security problems in IT systems.

“If you think cryptography will solve your problem, then you don’t understand cryptography $\cdots$ and you don’t understand your problem."

The End

Thanks a lot for your attention!