Introduction to Cryptography

Dhananjoy Dey

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

January 3, 2024

Disclaimers

1

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

2

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.

3

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

Outline

Cryptology

Cryptology

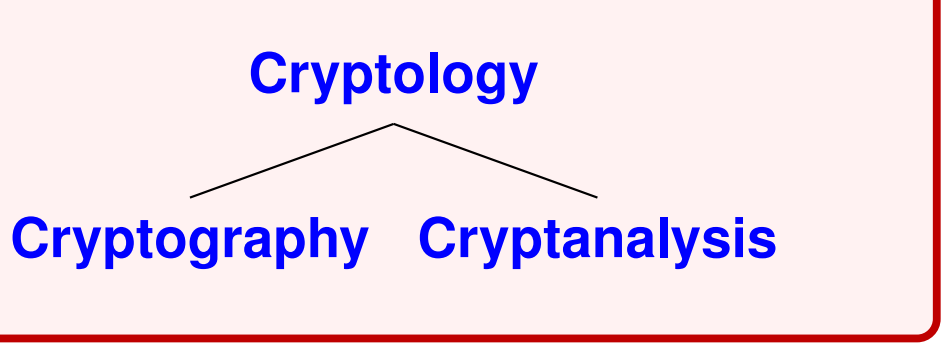
Cryptology

Cryptology

Cryptography **Cryptanalysis**

Cryptology

Cryptology

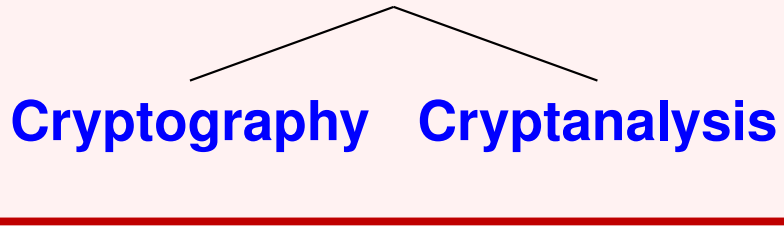


Cryptology

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

Cryptology

Cryptology

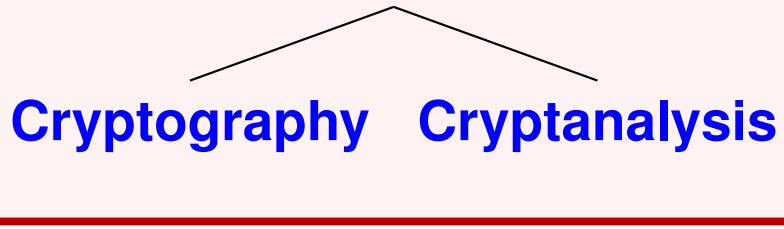


Cryptology

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

Cryptology

Cryptology

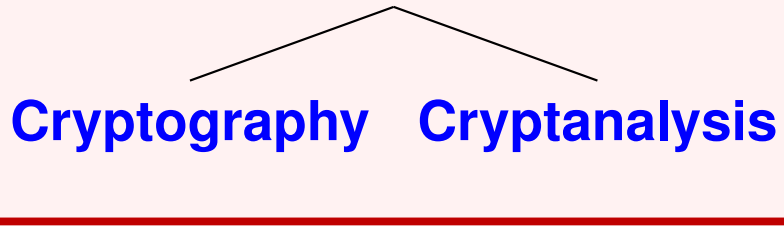


Cryptology

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

Cryptology

Cryptology



Cryptology

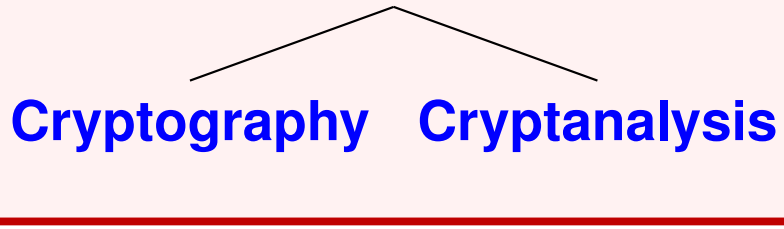
- **Cryptography:** is a science which deals with how to achieve '**PAIN**'
  '**P**rivacy' & Confidentiality
  Authentication,
  Integrity &
  Non-repudiation.
- **Cryptanalysis:** is a science which deals with how to defeat of achieving '**PAIN**'

Cryptography is about communication in the presence of an adversary.

— Rivest

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**'

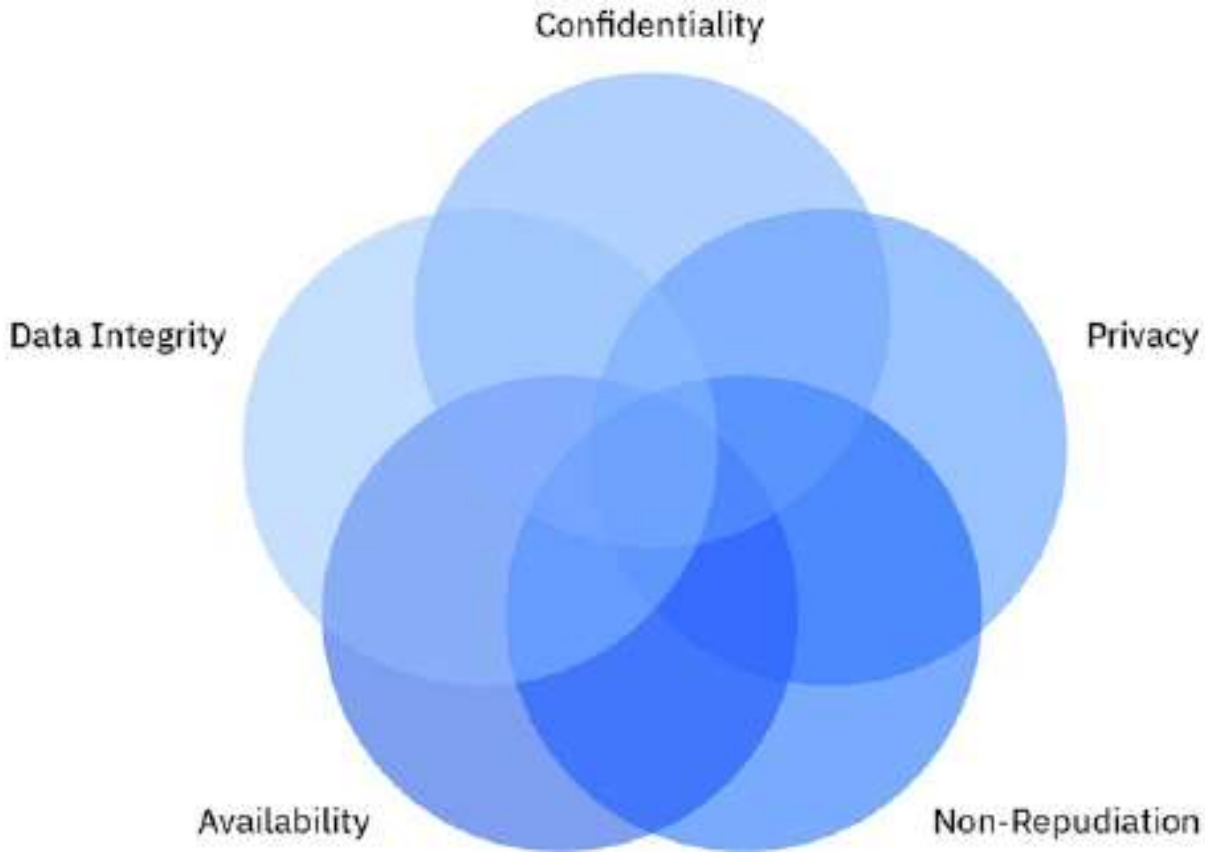
Cryptography is about communication in the presence of an adversary.

— Rivest

The Concise Oxford English Dictionary defines cryptography as "the art of writing or solving codes."

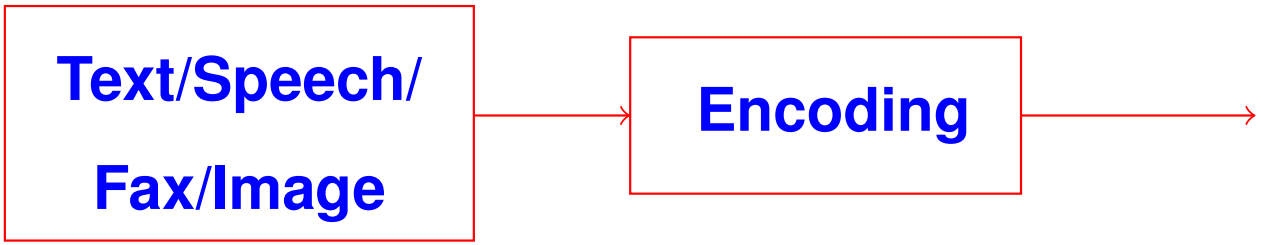
Cryptography

Cryptography supports multiple goals

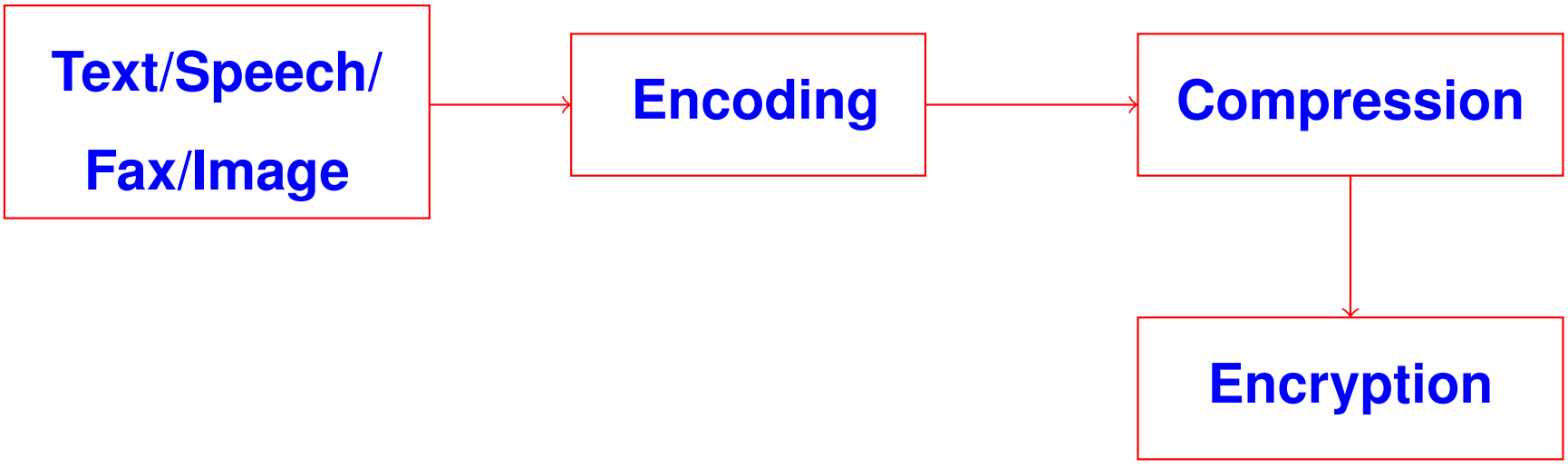


Cryptography for Secure Communication

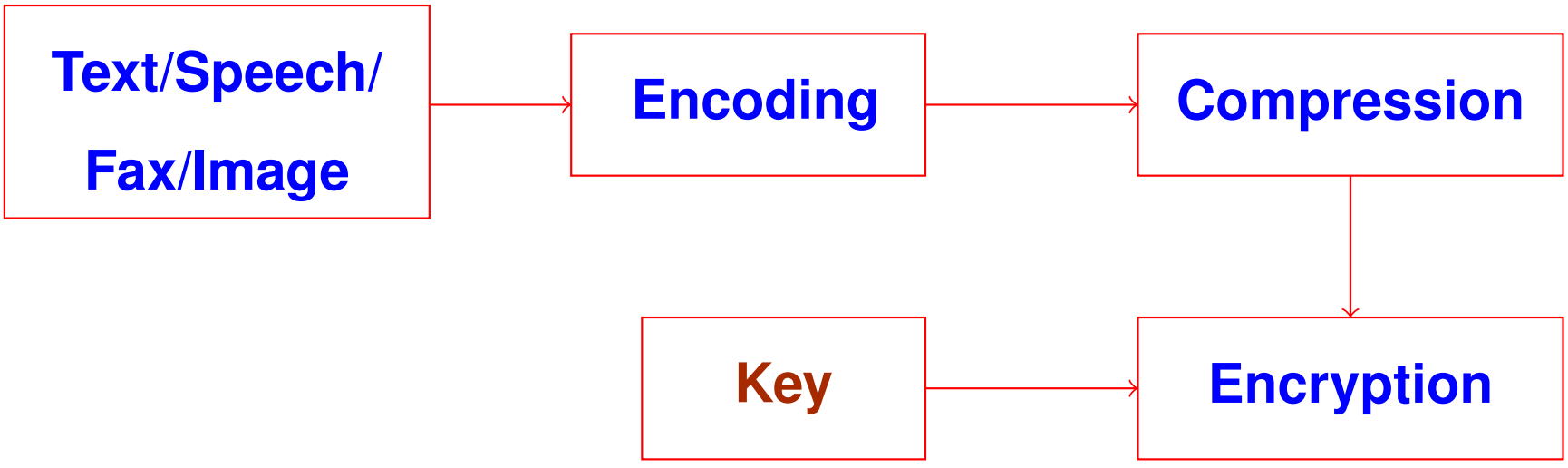
Cryptography for Secure Communication



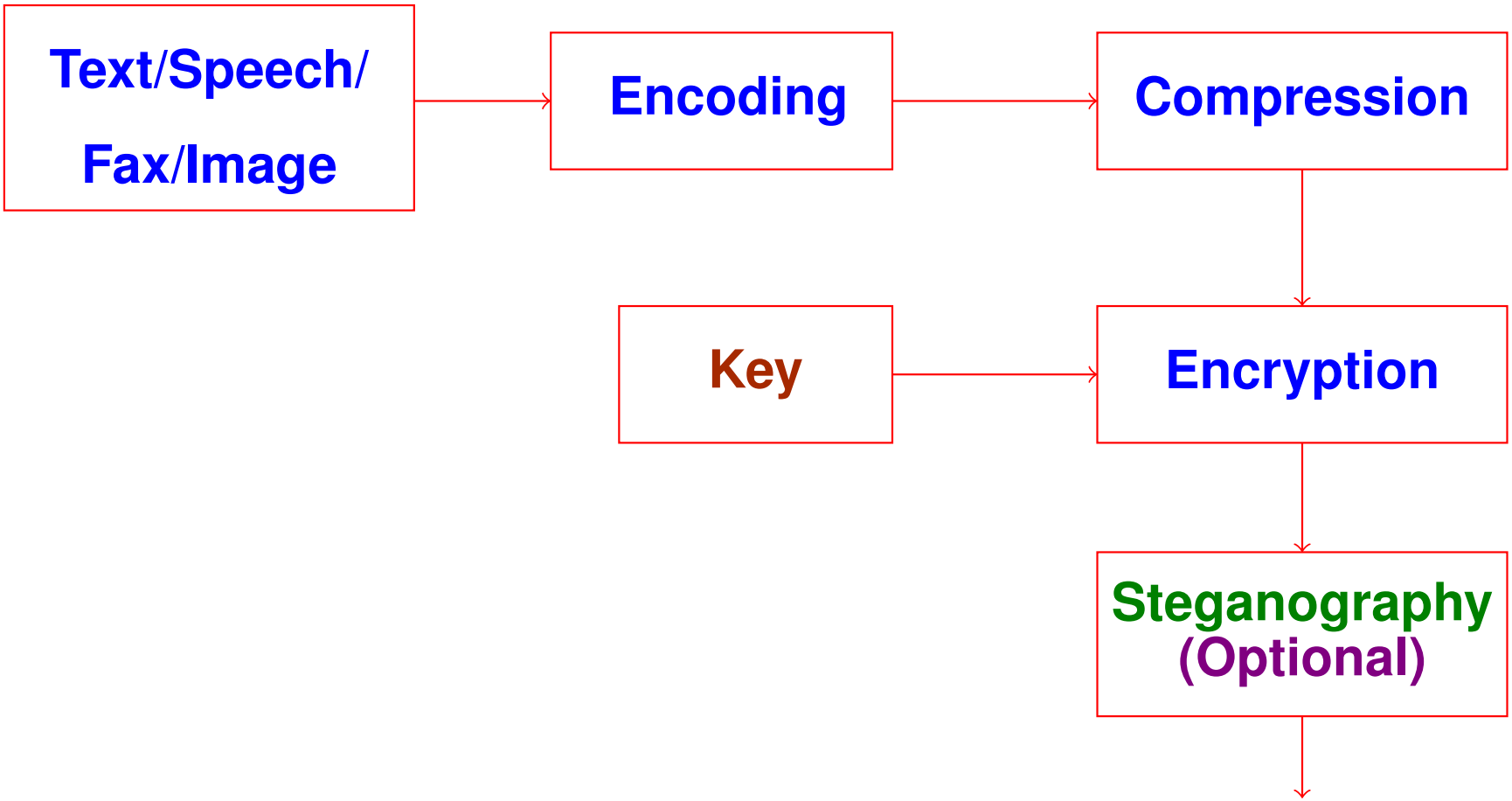
Cryptography for Secure Communication



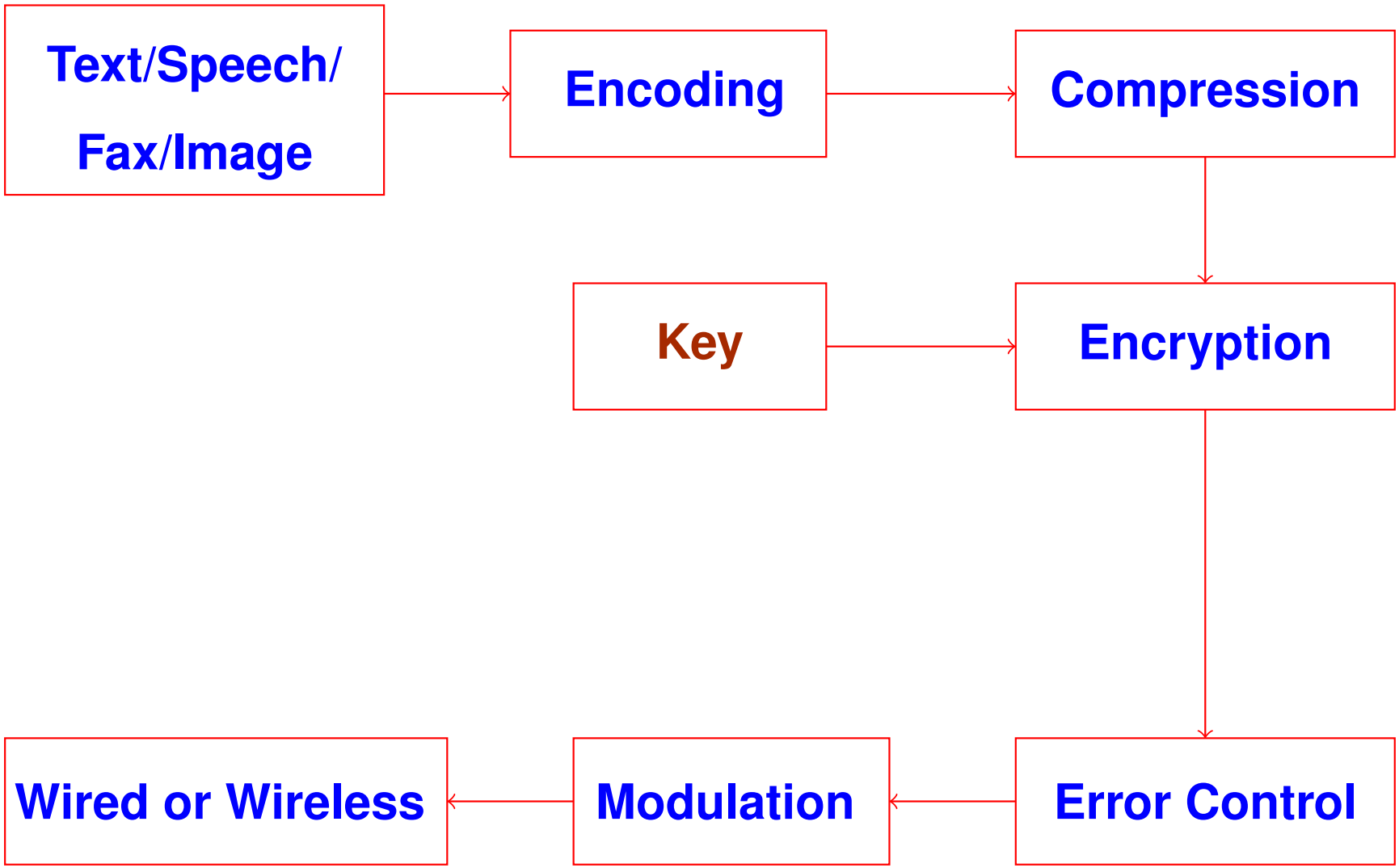
Cryptography for Secure Communication



Cryptography for Secure Communication



Cryptography for Secure Communication



Cryptography vs. Security

- Information security includes the study of subjects like:
  - Computer security
  - Network security
  - Software security

Cryptography vs. Security

- Information security includes the study of subjects like:
  - Computer security
  - Network security
  - Software security
- Cryptography provides some mathematical tools that can assist with the provision of information security services. It is a small but essential part of a complete solution.

Cryptography vs. Security

- Information security includes the study of subjects like:
  - Computer security
  - Network security
  - Software security
- Cryptography provides some mathematical tools that can assist with the provision of information security services. It is a small but essential part of a complete solution.
- Security is a chain
  - Weak links become targets
  - One flaw is all it takes

Cryptography vs. Security

- Information security includes the study of subjects like:
  - Computer security
  - Network security
  - Software security
- Cryptography provides some mathematical tools that can assist with the provision of information security services. It is a small but essential part of a complete solution.
- Security is a chain
  - Weak links become targets
  - One flaw is all it takes (Door locks $\neq$ Home security)
  - Cryptography is usually not the weakest link (however, when the crypto fails the damage can be catastrophic)

10 Cyber-security Domains

Information Security & Risk Management	Business Continuity & Disaster Recovery	Security Architecture & Design
Access Control	Physical & Environmental Security	Telecommunications & Network Security
Cryptography	Legal, Regulations, Compliance & Investigations	Application Security
...	Operations Security	...

Table: International Information Systems Security Consortium's 10 Domains

G. J. Touhill & C. J. Touhill,
Cyber-security for Executives: A Practical Guide, Wiley, 2014.

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

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

Cryptosystems

Definition

A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where

(i) $\mathcal{P}$ *is a finite set of possible plaintexts,*

(ii) $\mathcal{C}$ *is a finite set of possible ciphertexts,*

(iii) $\mathcal{K}$*, the keyspace, is a finite set of possible keys,*

(iv) *For each $K \in \mathcal{K}$, there is an encryption rule $e_K \in \mathcal{E}$ and a corresponding decryption rule $d_K \in \mathcal{D}$. Each*

$$e_K : \mathcal{P} \to \mathcal{C} \quad \text{and} \quad d_K : \mathcal{C} \to \mathcal{P}$$

are functions s/t

$$d_K(e_K(x)) = x$$

for every plaintext element $x \in \mathcal{P}$.

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.

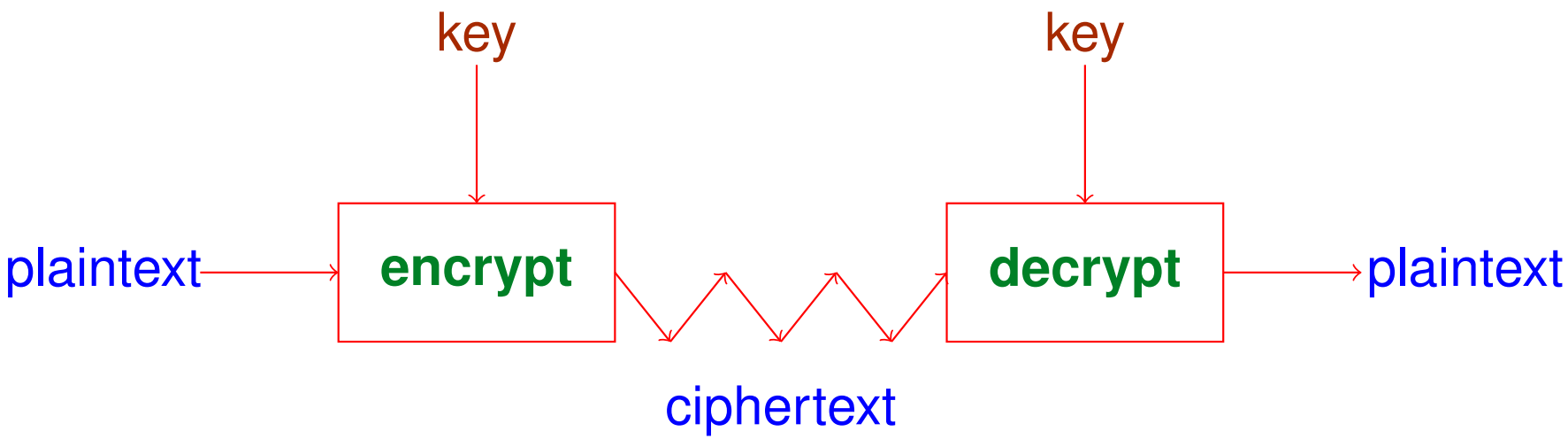
Requirements for Good Cryptosystems

- 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.

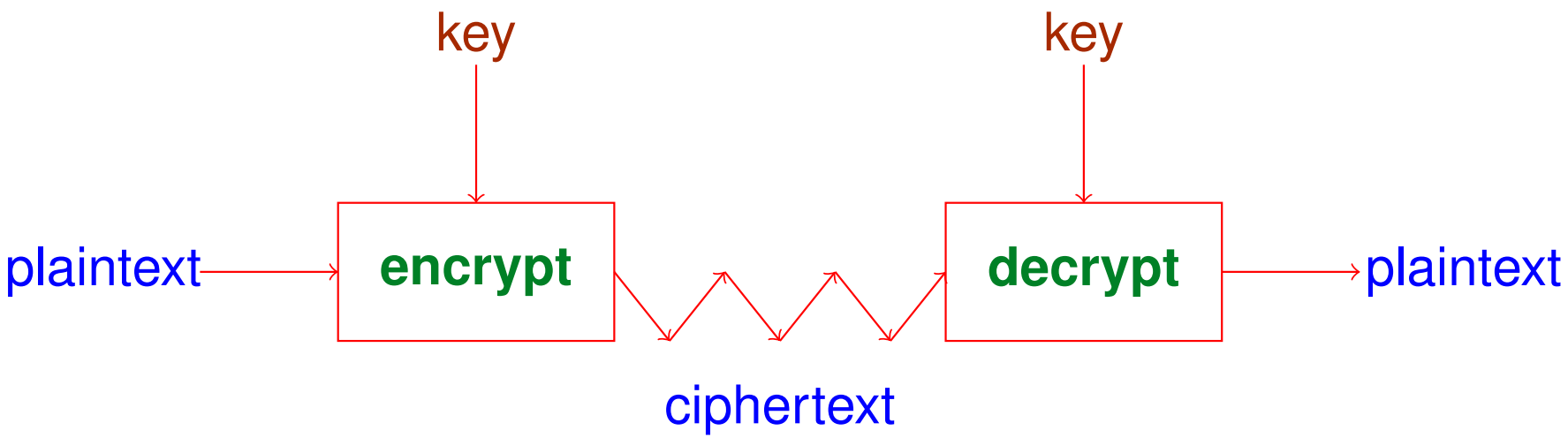
Requirements for Good Cryptosystems

- 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

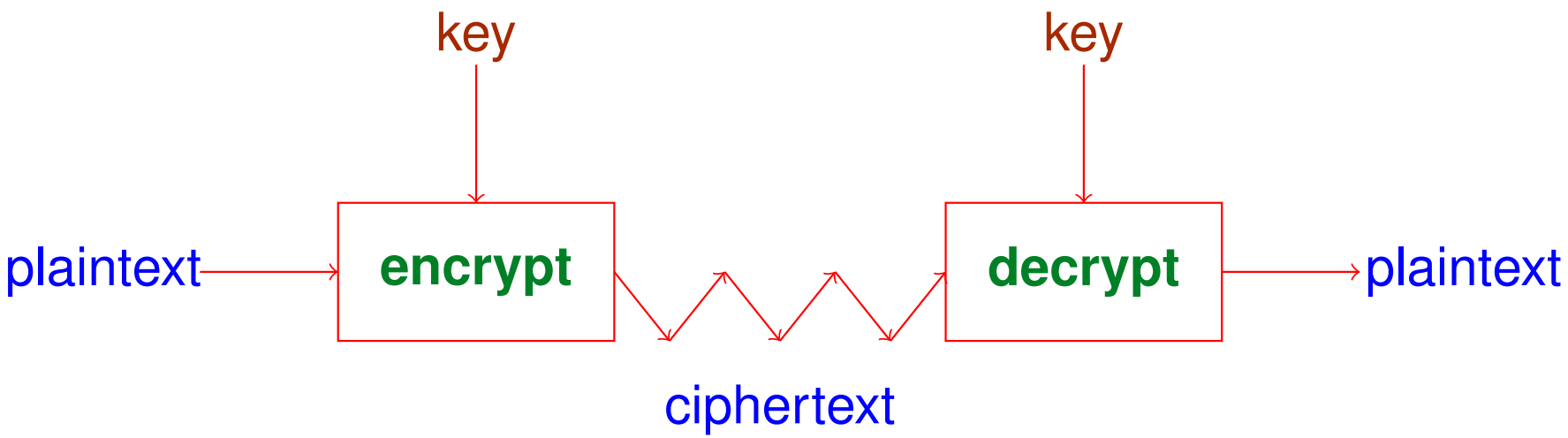


A Generic View of Secret Key Crypto



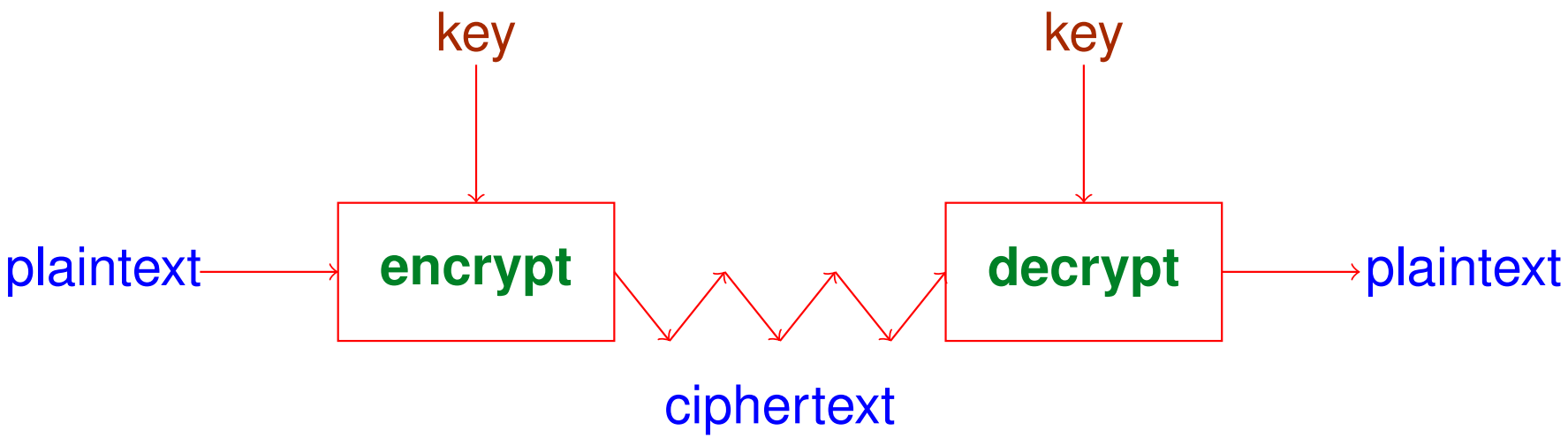
- Sender and receiver use the same key
- Sender and receiver are equivalent
- The oldest type of cryptography
- Gives the best performance
- Provides highest security standards

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



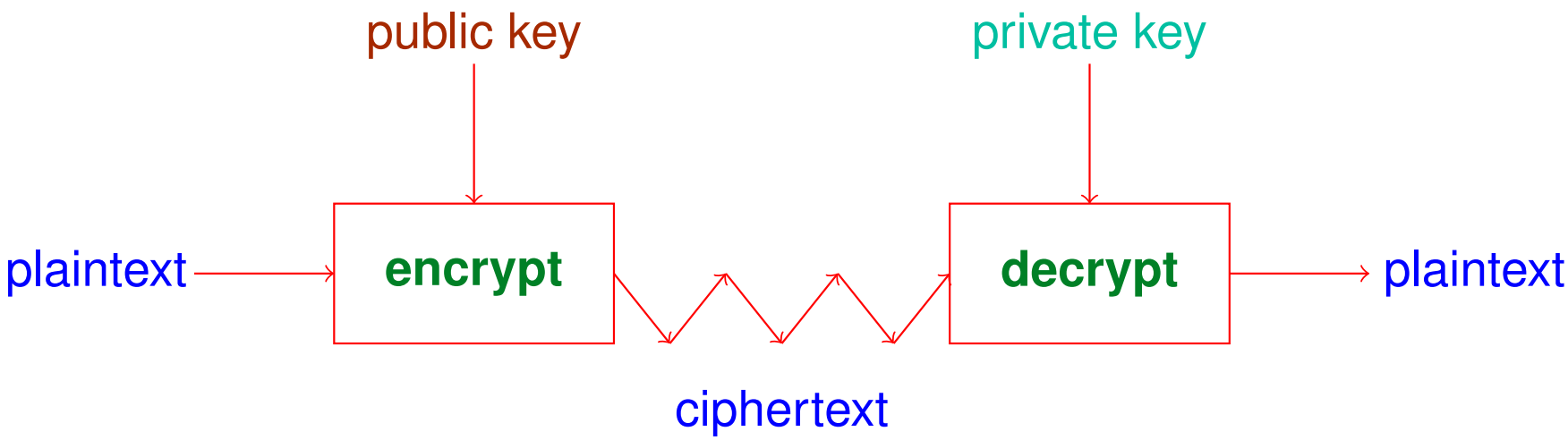
- Sender and receiver use the same key
- Sender and receiver are equivalent
- The oldest type of cryptography
- Gives the best performance
- Provides highest security standards
- Only disadvantage: difficult key management

Secret Key Crypto

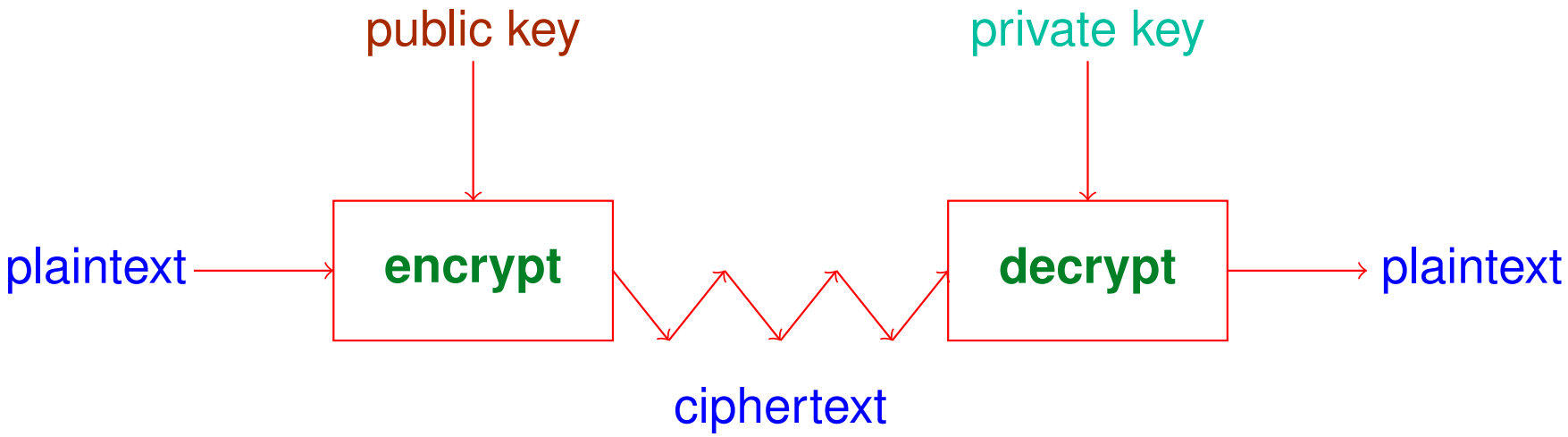
Classification

Secret Key Cryptography

A Generic View of Public Key Crypto



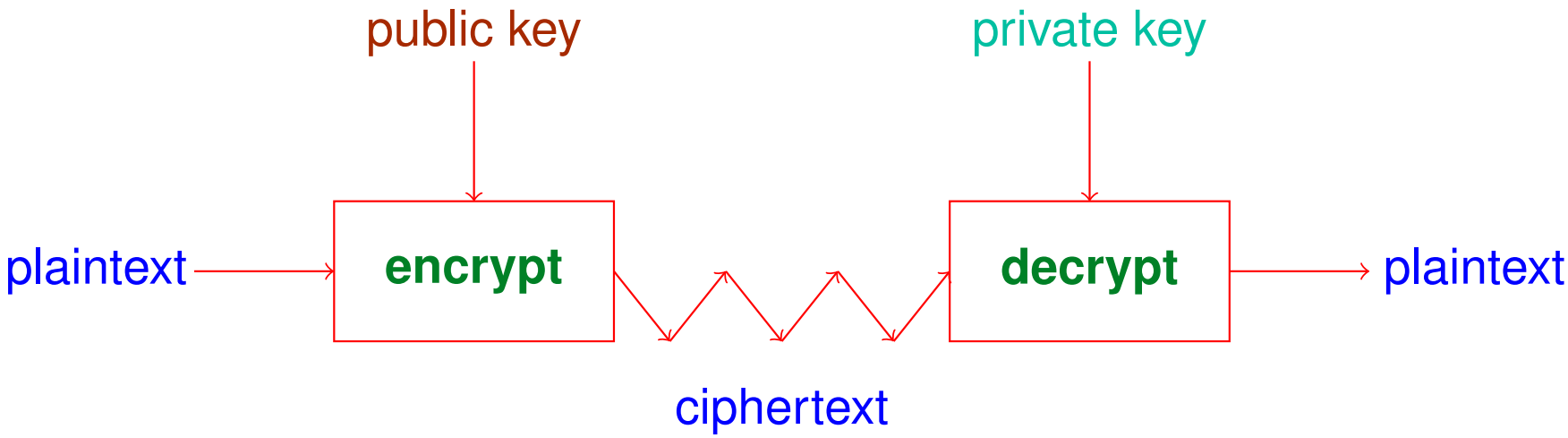
A Generic View of Public Key Crypto



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

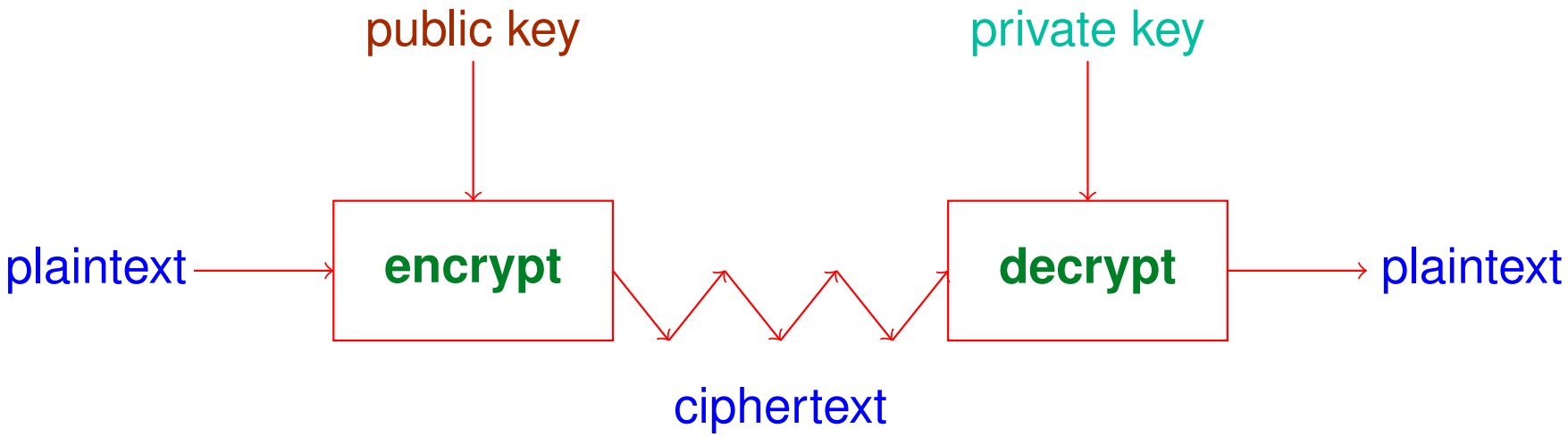


Advantages over symmetric-key

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



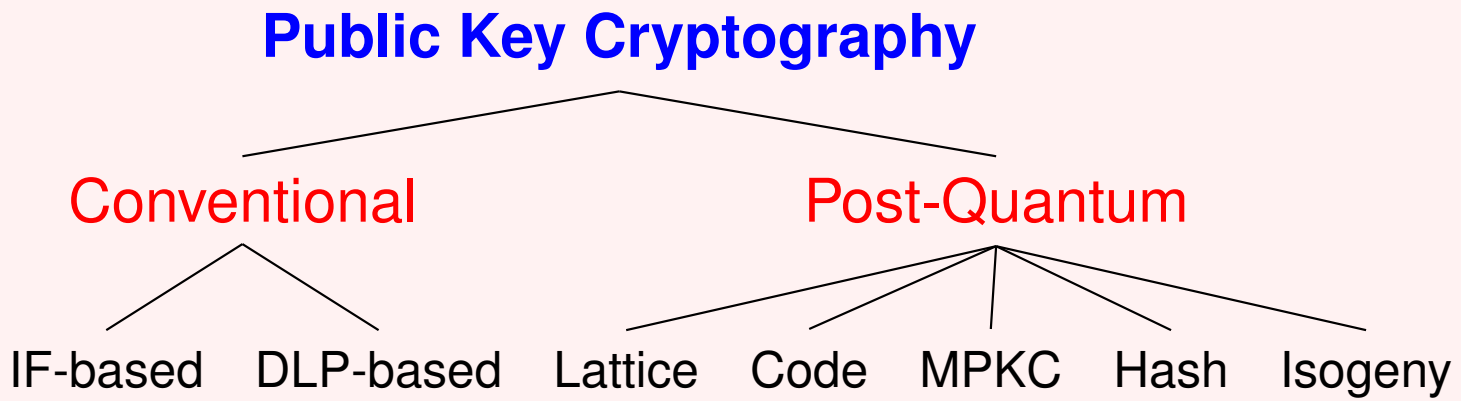
Advantages over symmetric-key

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



Hybrid Cryptography

- **Drawback of PKC**
  - much slower than secret-key Crypto
- **Drawback of secret-key Crypto**
  - key management

Hybrid Cryptography

- **Drawback of PKC**
  - much slower than secret-key Crypto
- **Drawback of secret-key Crypto**
  - key management
- **Hybrid cryptography:** to take the benefits of both
  - Apply PKC to encrypt the the 'secret key' k
  - Use 'secret key' k to encrypt the message M

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

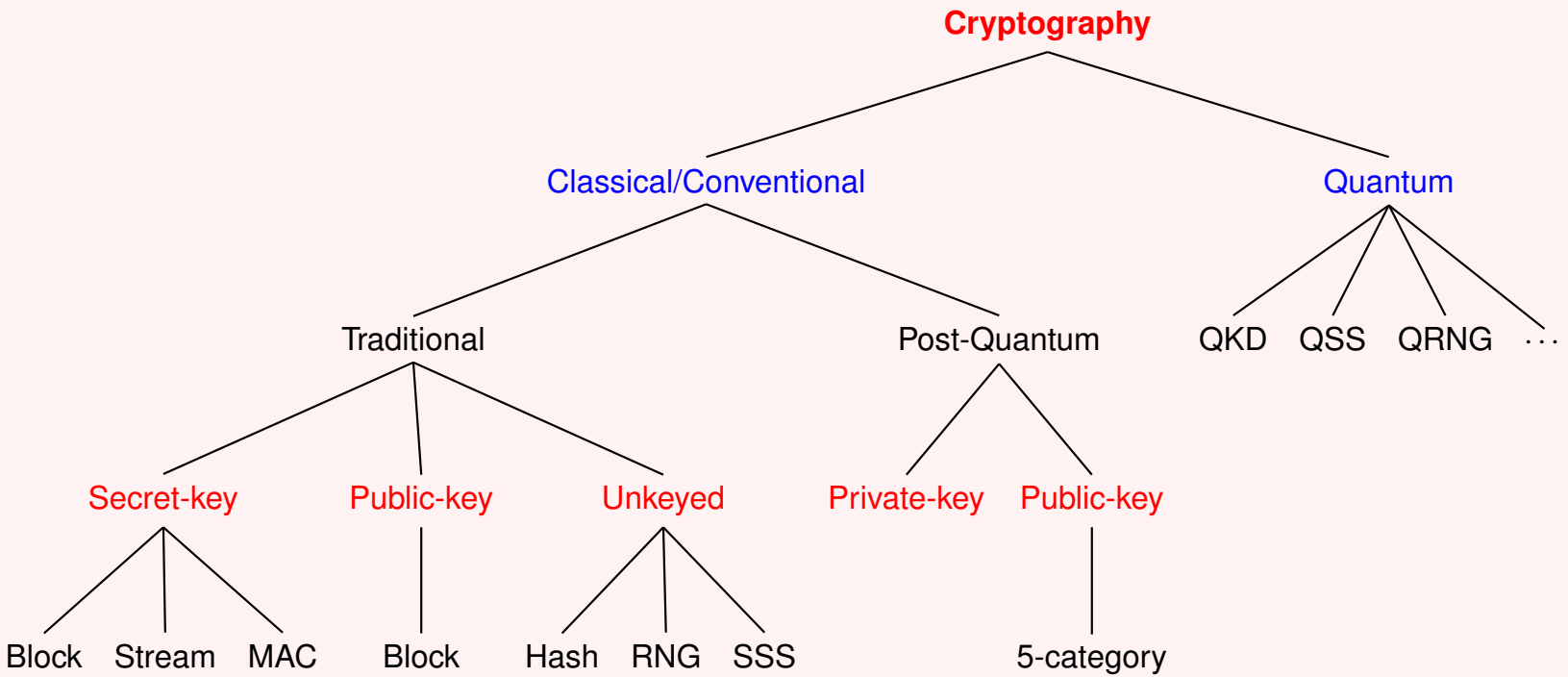
- Basic assumptions:
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms are not secret
- This is known as *Kerckhoffs' Principle*

- 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?

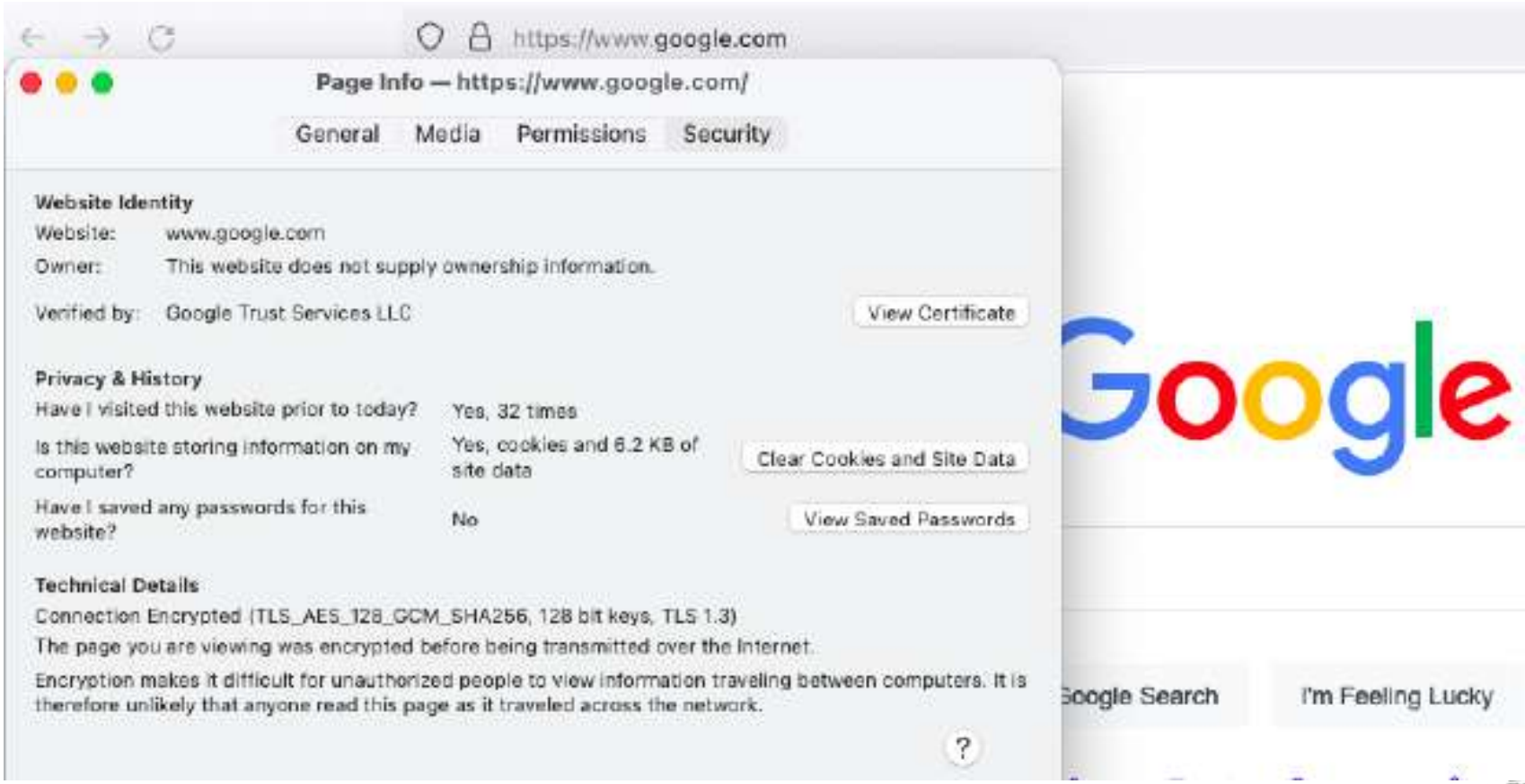
Classification of Cryptography

Classification of Cryptography

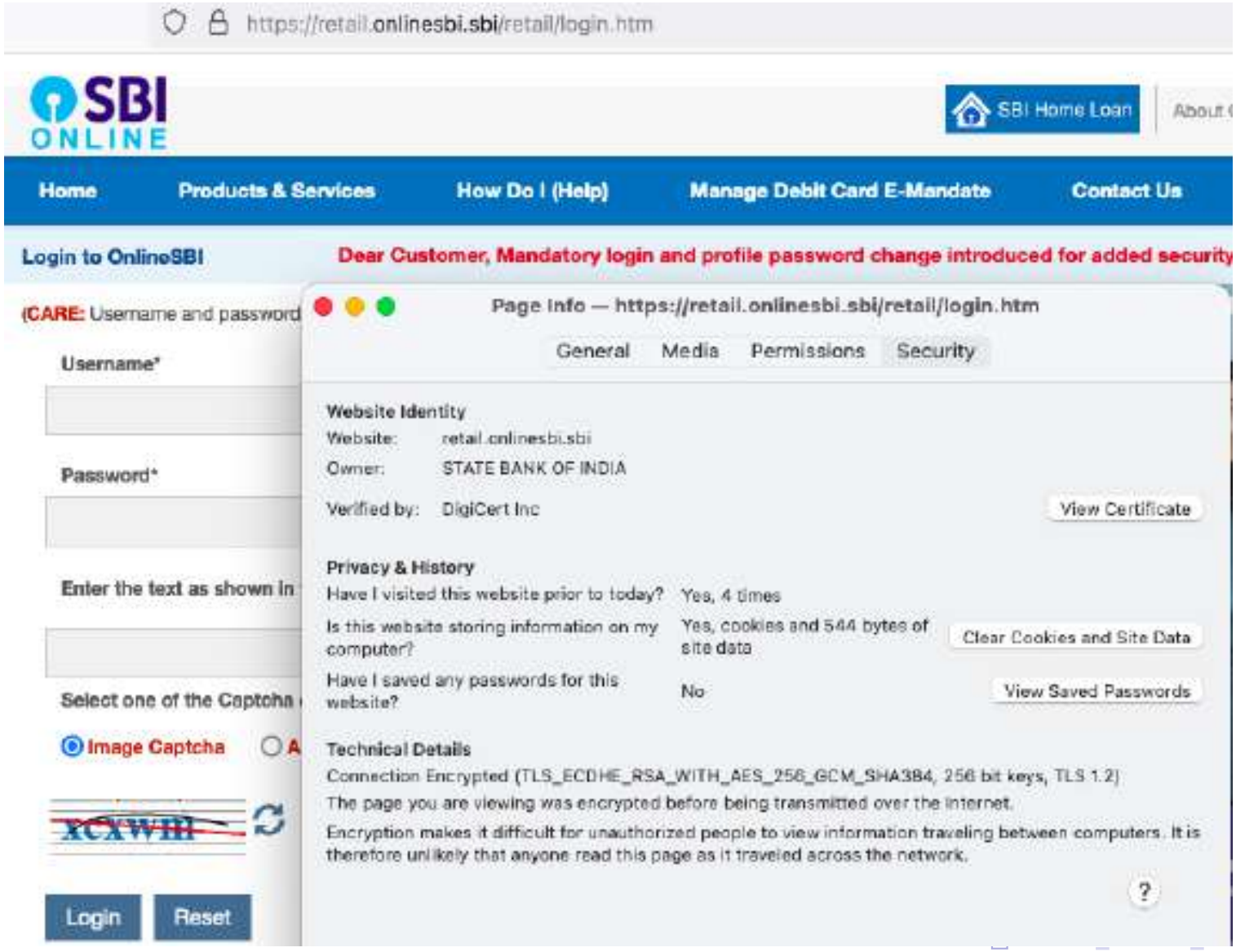
Classification



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

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

Cryptography is Everywhere

Figure: e-KYC Service Provided by the UIDAI

- $SHA\text{-}256(\textit{the KYC data})$ 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

- $SHA\text{-}256(the\ KYC\ data)$ 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, . . .)
- . . .

Home > Insights > Quantum Cryptography: The Future of Secure Digital Payments

Quantum Cryptography: The Future of Secure Digital Payments

18-07-2023 | By Liam Critchley

Digital payments and digital banking have become more and more popular over the last decade or so and have replaced cash transactions in many parts of society. The adoption of online banking and digital payments was also accelerated during the COVID-19 pandemic when most transactions involved no cash at all in preventing viral transmission.

While physical money is not obsolete, it is less commonly used in many parts of the world (especially the Western world). If society is to switch to digital payments being the main way of paying, then they need to have a similar level of security as physical payments—especially being tamper-resistant and untraceable. However, digital payments also need an extra layer of security because, unlike physical notes, digital payments are susceptible to digital attackers and data breaches, so digital payment providers need to be more vigilant in the prevention of cyberattacks.

https://www.electropages.com/blog/2023/07/future-digital-payments-deep-dive-quantum-cryptography

https://fagenwasanni.com/news/post-quantum-cryptography-a-decade-of-revolutionizing-internet-security/54458/

Researchers Find 'Backdoor' in Encrypted Police and Military Radios

The TETRA standard is used in radios worldwide. Security researchers have found multiple vulnerabilities in the underlying cryptography and its implementation, including issues that allow for the decryption of traffic.

By Joseph Cox

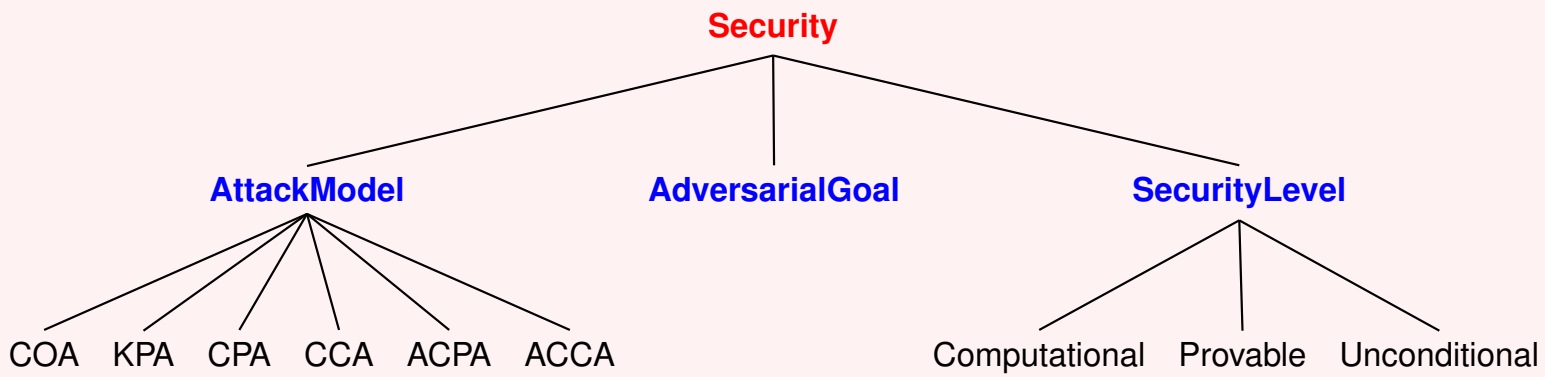
24 July 2023, 3:30pm Share Tweet Snap

https://www.vice.com/en/article/4a3n3j/backdoor-in-police-radios-tetra-burst

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."

Outline

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

Course Contents – Cryptography

- **Public-Key Cryptography**
  - Diffie-Hellman Key Exchange
  - The RSA Cryptosystem
  - The ElGamal Cryptosystem
  - Elliptic Curves Cryptosystem
  - Digital Signature Schemes
- **Key Establishment**

References

- **Textbook**
  - J. Katz & Y. Lindell,
    Introduction to Modern Cryptography, CRC Press, 2021.
  - D. R. Stinson & M. B. Paterson,
    Cryptography – Theory and Practice, CRC, 2019.

References

- **Supplementary Reading**


William Easttom,
Modern Cryptography: Applied Mathematics for Encryption and Information Security, Springer, 2021.


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.


William Stallings,
Cryptography and Network Security: Principles and Practice, Pearson Education Limited , 2023.


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

References

- National Institute of Standards and Technology
- ENISA – The European Union Agency for Cybersecurity
- KU Leuven
  – Research group COSIC, KU Leuven
- Inria

⋮

The End

Thanks a lot for your attention!