THREE- DAY WORKSHOP ON PUBLIC KEY INFRASTRUCTURE

DATE: 27th -29th MAY 2015

Centre for Development of Advanced Computing (C-DAC)
Bangalore

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Digital Signatures and PKI

Sanjay Adiwal
Centre for Development of Advanced Computing (C-DAC)
Bangalore

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

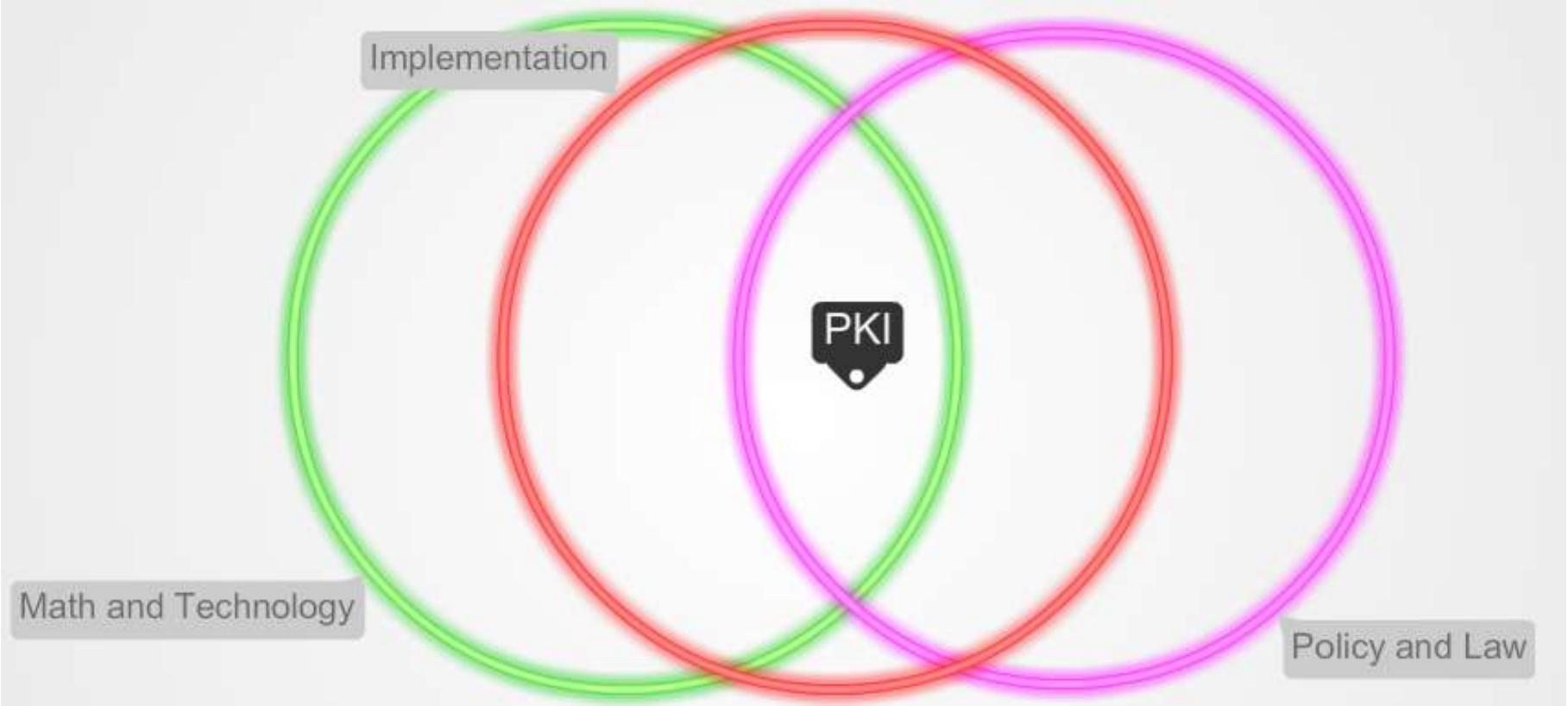
Agenda

- ✓ Dimensions of PKI
- ✓ Paper World Vs Electronic World
- ✓ Why Digital Signature?
- ✓ What is Digital Signature?
- ✓ Achieving Confidentiality
- ✓ What is Digital Signature Certificate?
- ✓ Certifying Authority & Trust Model
- ✓ Certificate Issuance, Types, Classes

PKI?

- A **public key infrastructure** (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Dimensions of PKI



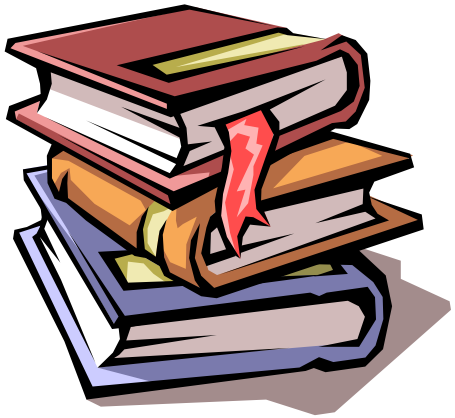
- PKI – Public Key Infrastructure ecosystem is an intersection of:
  - Cryptography (Math) & Technology – Cryptographers/Researchers
  - Policy & Law – PKI System & Users
  - Implementation – PKI System Developer

Technology Perspective

Paper Records v/s Electronic Records

Paper Records v/s Electronic Records

	Paper Record	Electronic Record
Document Form	Physical	Digital
Very easy to make copies	No	Yes
Very fast distribution	No	Yes
Archival and Retrieval	Challenging	Easy
Copies are as good as original	No. Copies are easily distinguishable	Yes
Easily modifiable	No	Yes
Environmental Friendly	No	Yes



Trust-worthiness in Transactions

The following properties must be assured:

Privacy (Confidentiality): Ensuring that only Authorized persons should read the Data/Message/Document

Authenticity: Ensuring that Data/Message/Document are genuine

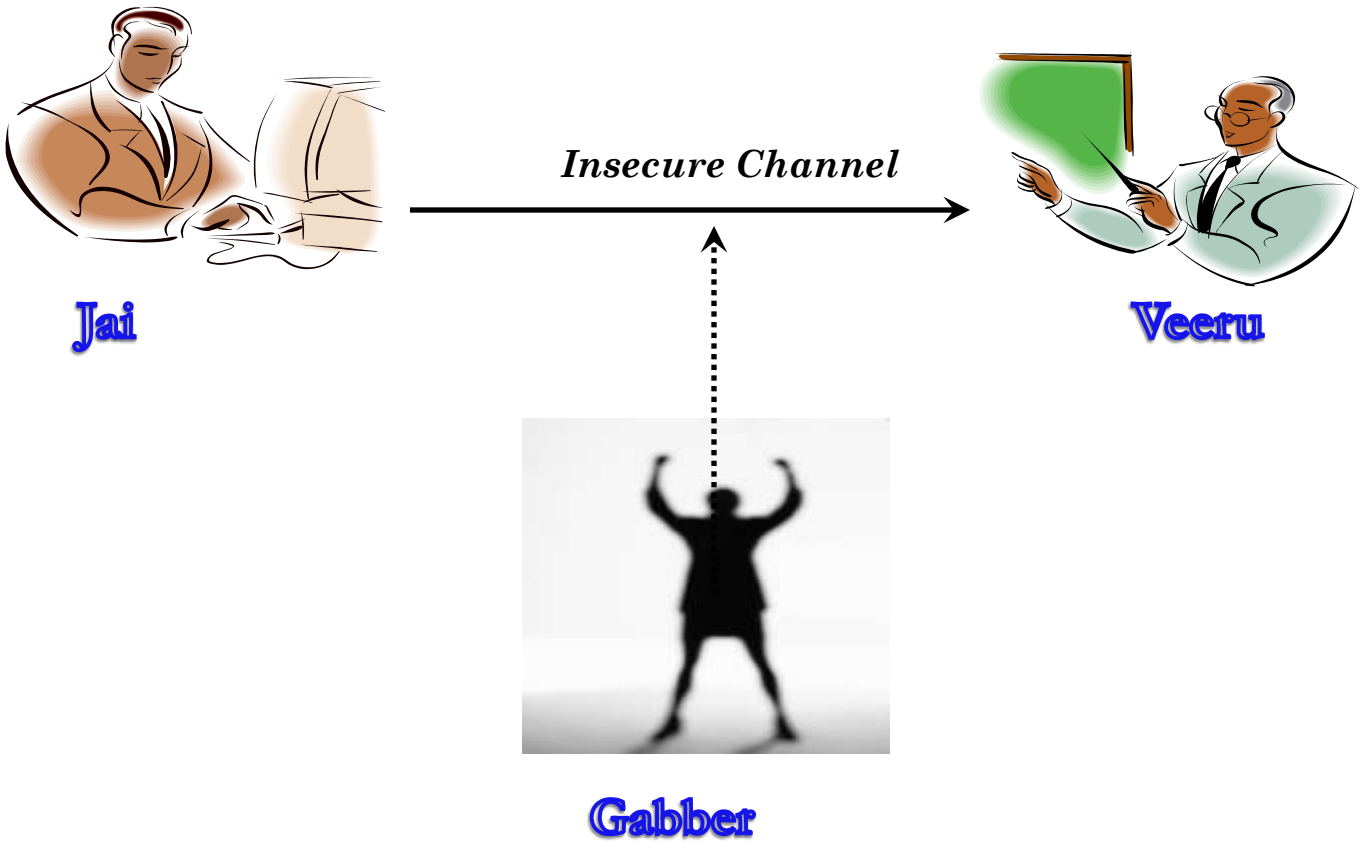
Integrity : Ensuring that Data/Message/Document are unaltered by unauthorized person during transmission

Non-Repudiation: Ensuring that one party of a transaction cannot deny having sent a message

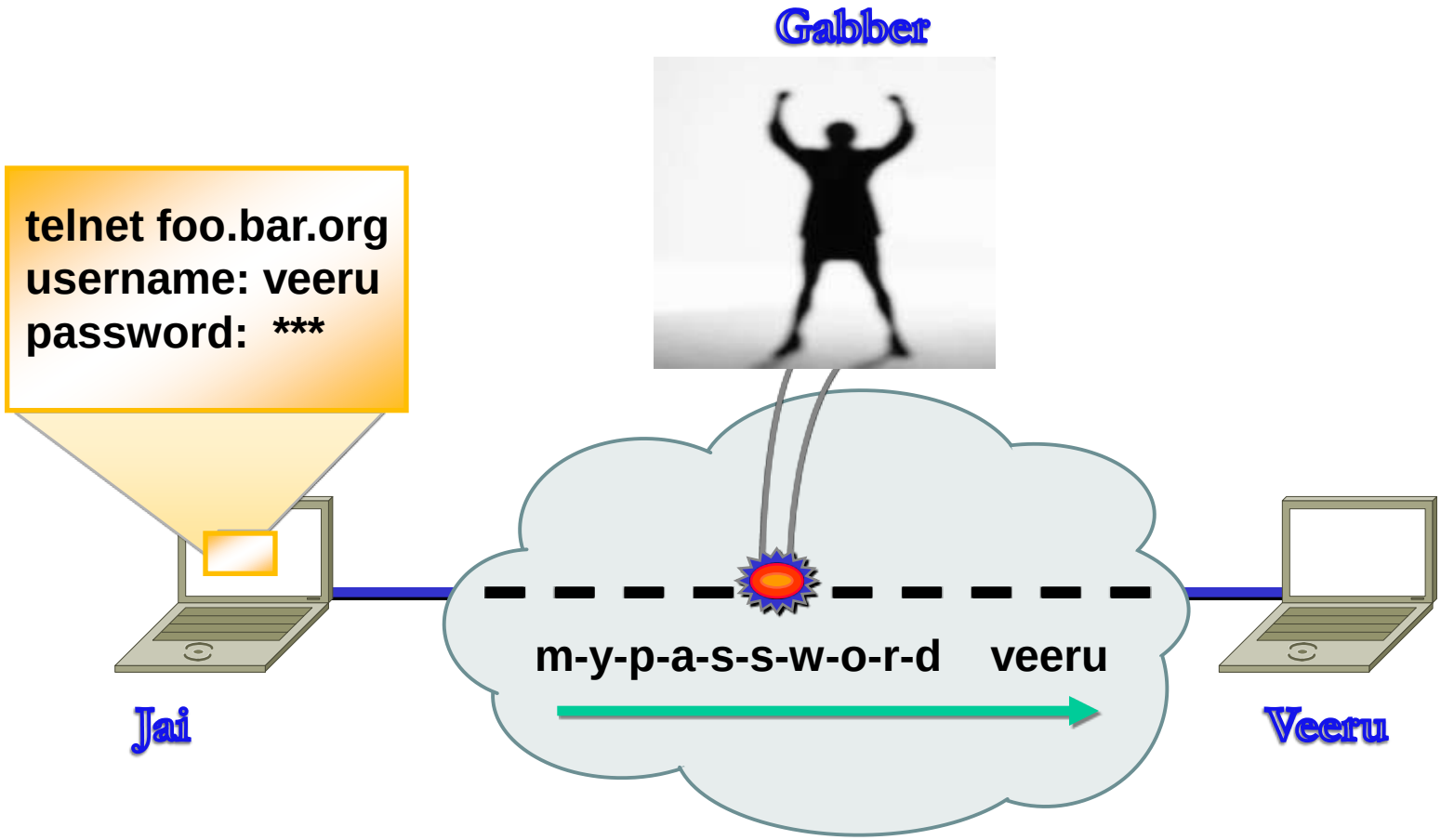
Paper Records v/s Electronic Records

	Paper Record	Electronic Record
Privacy (Confidentiality)	Sealed Envelope	Digital Envelope
Authenticity	Hand Signature	Digital Signature
Integrity	Hand Signature	Digital Signature
Non-Repudiation	Hand Signature but it is Challenging	Digital Signature

The Scenario

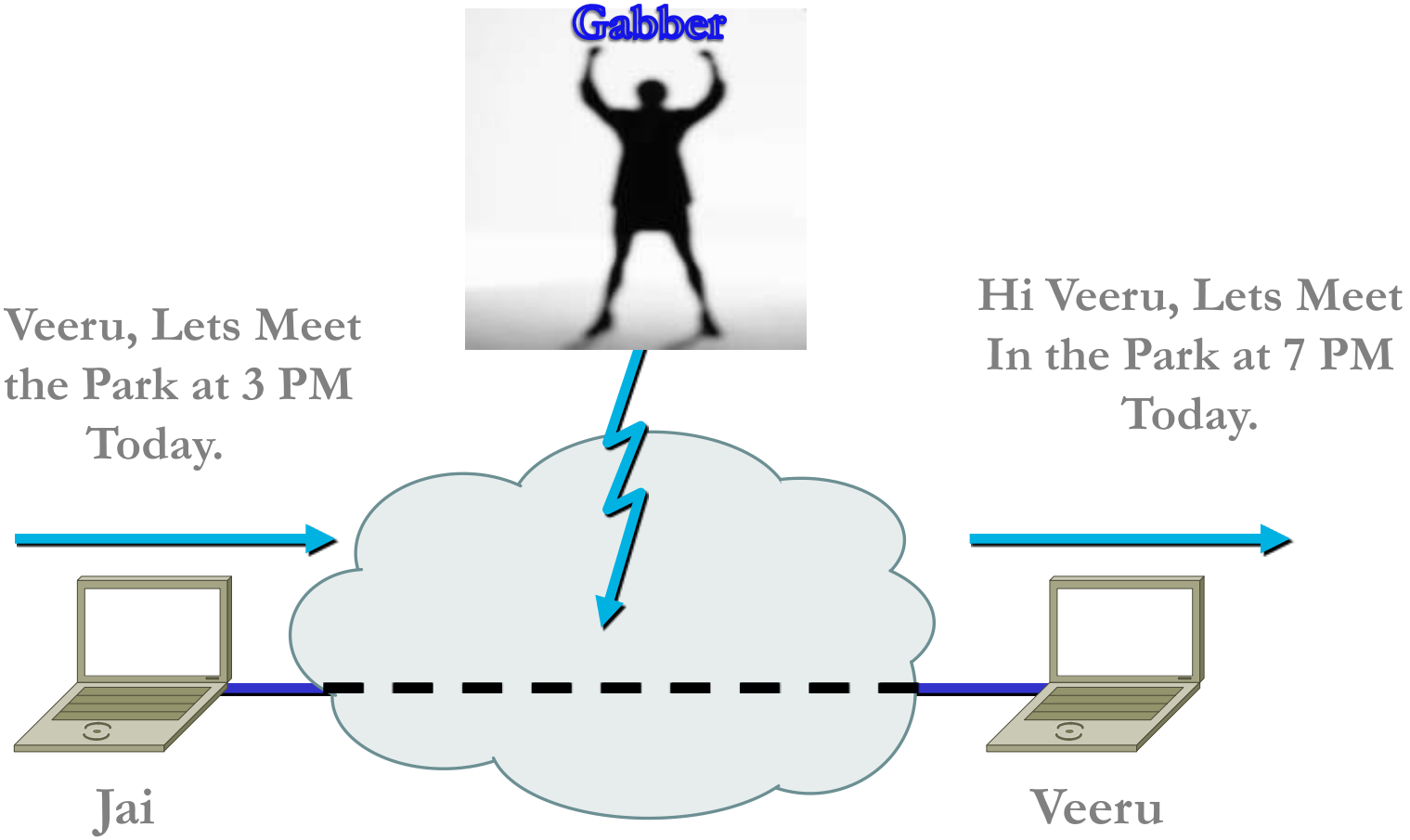


Threats: Packet Sniffing



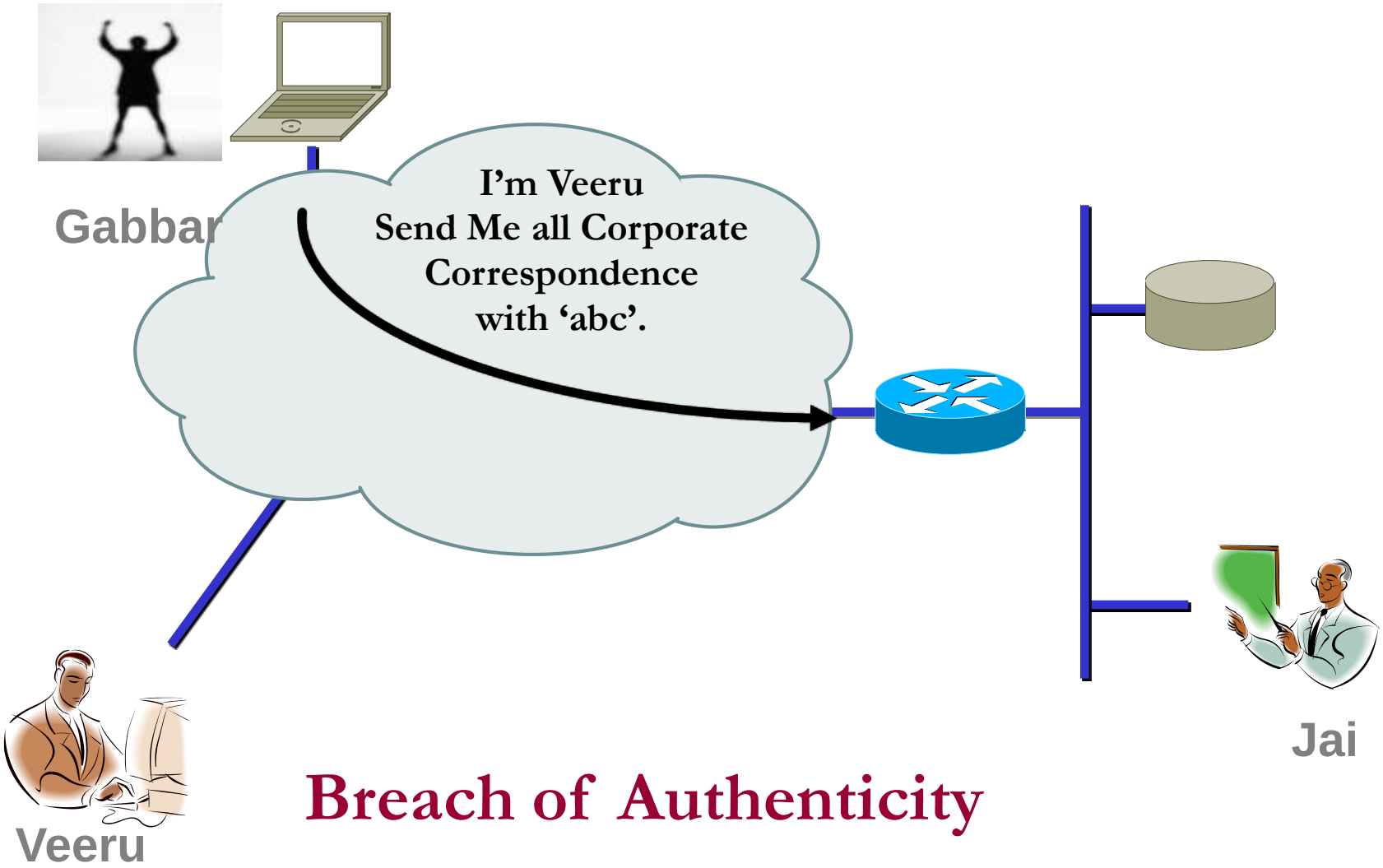
Breach of Confidentiality

Threats: Data Alteration



Breach of Integrity

Threats: Spoofing



Breach of Authenticity

Why Digital Signature?

Why Digital Signatures?

- To provide **Authenticity, Integrity and Non-repudiation** to electronic documents
- To enable the use of Internet as the safe and secure medium for e-Commerce and e-Governance

Mathematical Perspective

Major Components of Digital Signature

- Major cryptographic components for creating Digital Signature are:
  - Hash Functions
  - Asymmetric Key Cryptography

Hash Function

- A hash function is a cryptographic mechanism that operates as one-way function
  - Creates a digital representation or "fingerprint“ (Message Digest)
  - Fixed size output
  - Change to a message produces different digest

Examples : MD5 , Secure Hashing Algorithm (SHA)

Hash - Example

Message

Hi Jai,

I will be in the park at

3 pm

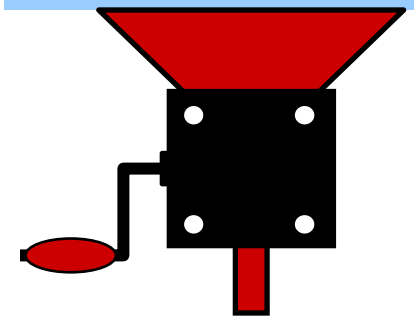
Veeru

Hi Jai,

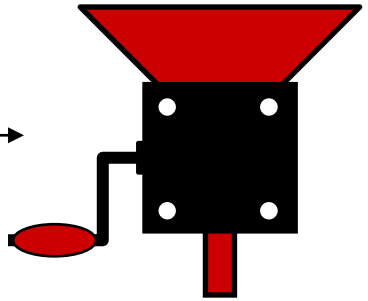
I will be in the park at

3 am

Veeru



← Hash Algorithm →



Message Digest

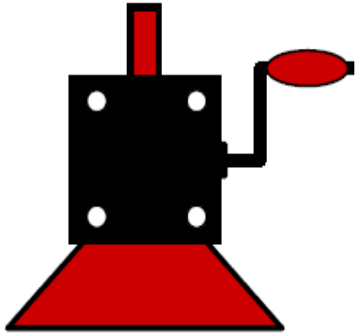
cfa2ce53017030315fde705b9382d9f4

d4216ytf6b9385fe502b165dfe8cec17

Digests are Different

Hash – One-way

cfa2ce53017030315fde705b9382d9f4



Hi Jai

I will be in the park at

3 pm

Veeru

MD5 and SHA

Message

Hi Jai,
I will be in the
park at 3 pm
Veeru

MD5

Message Digest

cfa2ce53017030315f
de705b9382d9f4

128 Bits

Hi Jai,
I will be in the
park at 3 pm
Veeru

SHA-1

1f695127f210144329ef
98e6da4f4adb92c5f18
2

160 Bits

Hi Jai,
I will be in the
park at 3 pm
Veeru

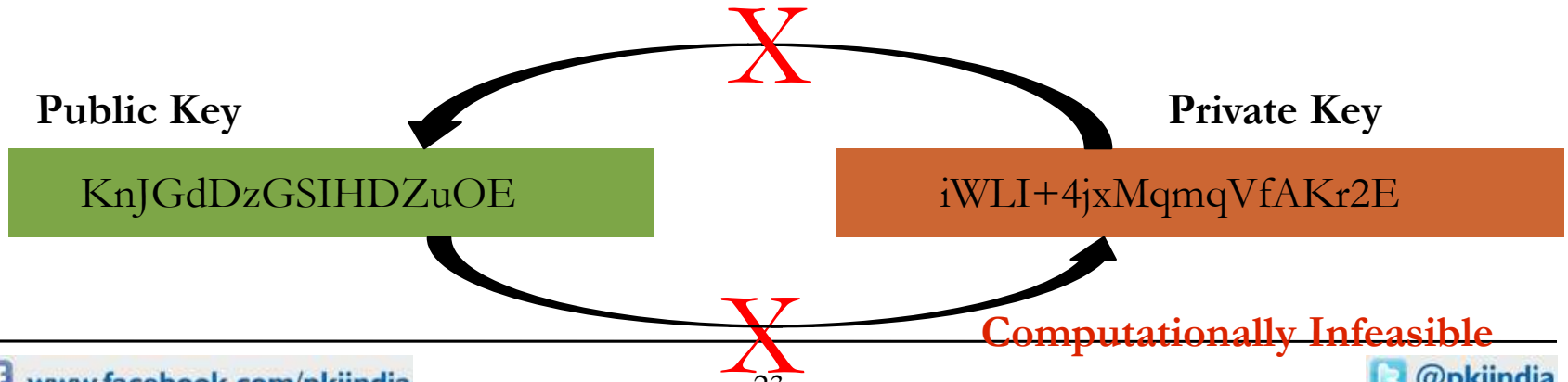
SHA-2

2g5487f56r4etert654tr
c5d5e8d5ex5gttahy55e

224/256/384/512

Asymmetric Key Cryptography

- Also called as Public Key Cryptography
- Uses a related key pair wherein one is Private key and another is Public key
  - One for encryption, another for decryption
- Knowledge of the *encryption* key doesn't give you knowledge of the *decryption* key
- A tool generates a related key pair (public & private key)



RSA Key pair

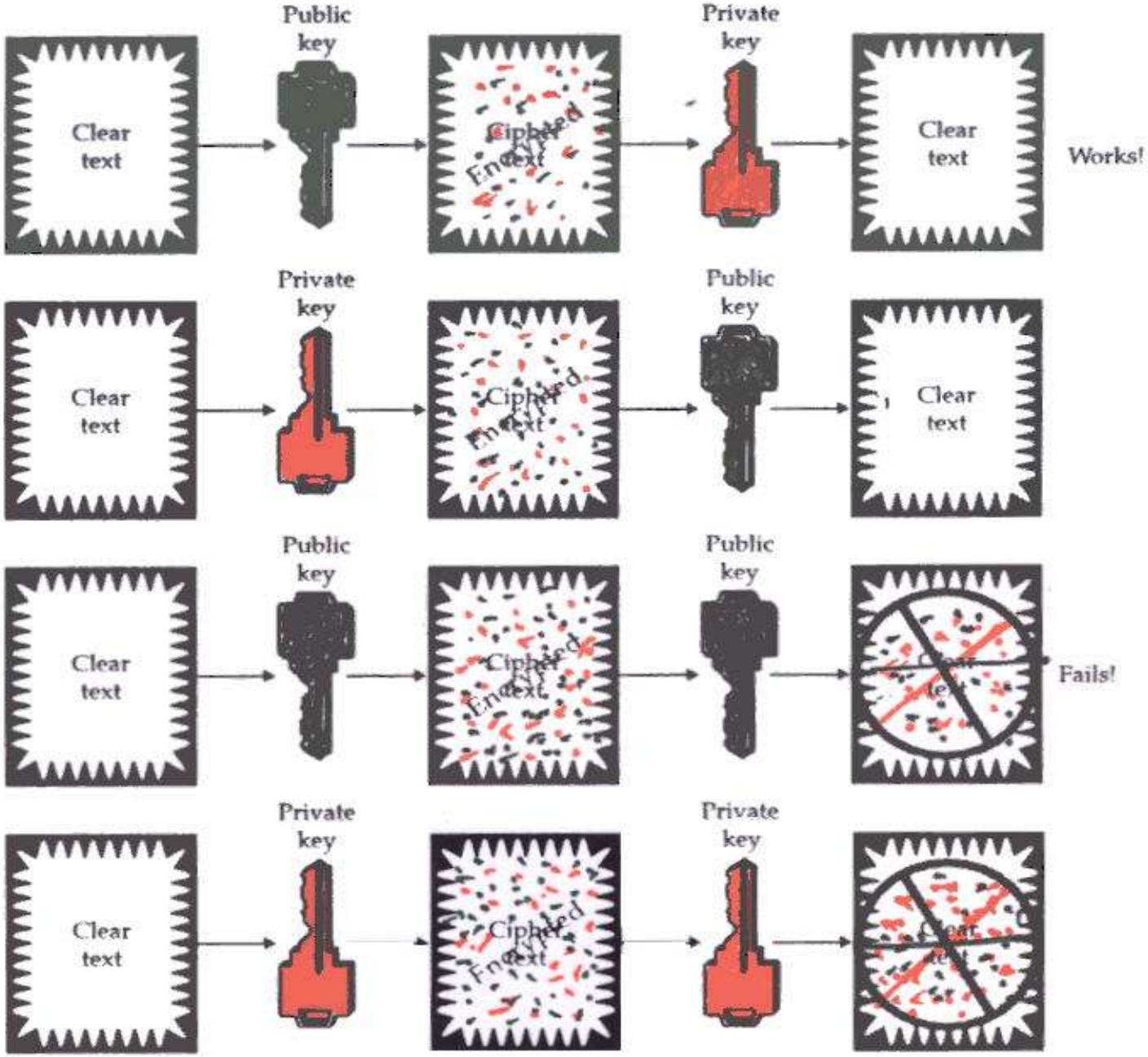
(including Algorithm identifier) [2048 bit]

Private Key

```
3082 010a 0282 0101 00b1 d311 e079 5543 0708 4ccb 0542 00e2 0d83
463d e493 bab6 06d3 0d59 bd3e c1ce 4367 018a 21a8 efbc ccd0 a2cc
b055 9653 8466 0500 da44 4980 d854 0aa5 2586 94ed 6356 ff70 6ca3
a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1 463d 1ef0 b92c 345f
8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5 b35f
5a22 97ec 199b c105 68fd e6b7 a991 942c e478 4824 1a25 193a eb95
9c39 0a8a cf42 b2f0 1cd5 5ffb 6bed 6856 7b39 2c72 38b0 ee93 a9d3
7b77 3ceb 7103 a938 4a16 6c89 2aca da33 1379 c255 8ced 9cbb f2cb
5b10 f82e 6135 c629 4c2a d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742
859d 32a8 f92a 54fb ff78 41bc bd71 28f4 bb90 bcff 9634
```

Public Key

```
3082 01e4 f267 0142 0f61 dd12 e089 5547 0f08 4ccb 0542 00e2 0d83 463d
e493 bab6 0673 0d59 bf3e c1ce 4367 012a 11a8 efbc ccd0 a2cc b055 9653
8466 0500 da44 4980 d8b4 0aa5 2586 94ed 6356 ff70 6ca3 a119 d278 be68
2a44 5e2f cfcc 185e 47bc 3ab1 463d 1df0 b92c 345f 8c7c 4c08 299d 4055
eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b c105 68fd
e6b7 a991 942c e478 4824 1a25 193a eb95 9c39 0a8a cf42 b250 1cd5 5ffb
6bed 6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16 6c89 2aca
da33 1379 c255 8ced 9cbb f2cb 5b10 f82e 6135 c629 4c2a d02a 63d1 6559
b4f8 cdf9 f400 84b6 5742 859d 32a8 f92a 54fb ff78 41bc bd71 28f4 bb90
bcff 9634
```


Public key
Private key
Clear text
Ciphered text
Clear text
Works!
Private key
Public key
Clear text
Ciphered text
Clear text
Public key
Public key
Clear text
Ciphered text
Fails!
Private key
Private key
Clear text
Ciphered text

Matrix of Knowledge of Keys

Key details	*Jai* should know	*Veeru* should know
Jai's private key	Yes	No
Jai's public key	Yes	Yes
Veeru's private key	No	Yes
Veeru's public key	Yes	Yes

Implementation Perspective

Digital Signature

Hand Signature Vs Digital Signature

- A ***Hand Signature*** on a document is
  - a **unique pattern** dependant on some secret known only to the signer and
  - **Independent of the content** of the message being signed
- A ***Digital signature*** of a message is
  - **a number** dependent on some secret known only to the signer and
  - **Dependent on the content** of the message being signed
- Properties of Signatures
  - Must be verifiable
  - Provide Authentication
  - Provide Data Integrity
  - Provide Non-repudiation

What is Digital Signature?

- Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document
  - Digital Signature of a person therefore **varies from document to document** thus ensuring authenticity of each word of that document.
  - As the public key of the signer is known, anybody can verify the message and the digital signature

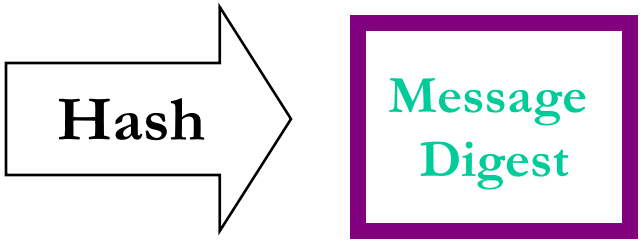
Creating Digital Signature

- Key pairs of every individual
  - ***Public key*** : known to everyone
  - ***Private key*** : known only to the owner
- To ***digitally sign*** an electronic document the signer uses his/her ***Private key***
- To ***verify*** a digital signature the verifier uses the signer's ***Public key***

Achieving **Authenticity**, **Integrity** and **Non-Repudiation** using Digital Signatures

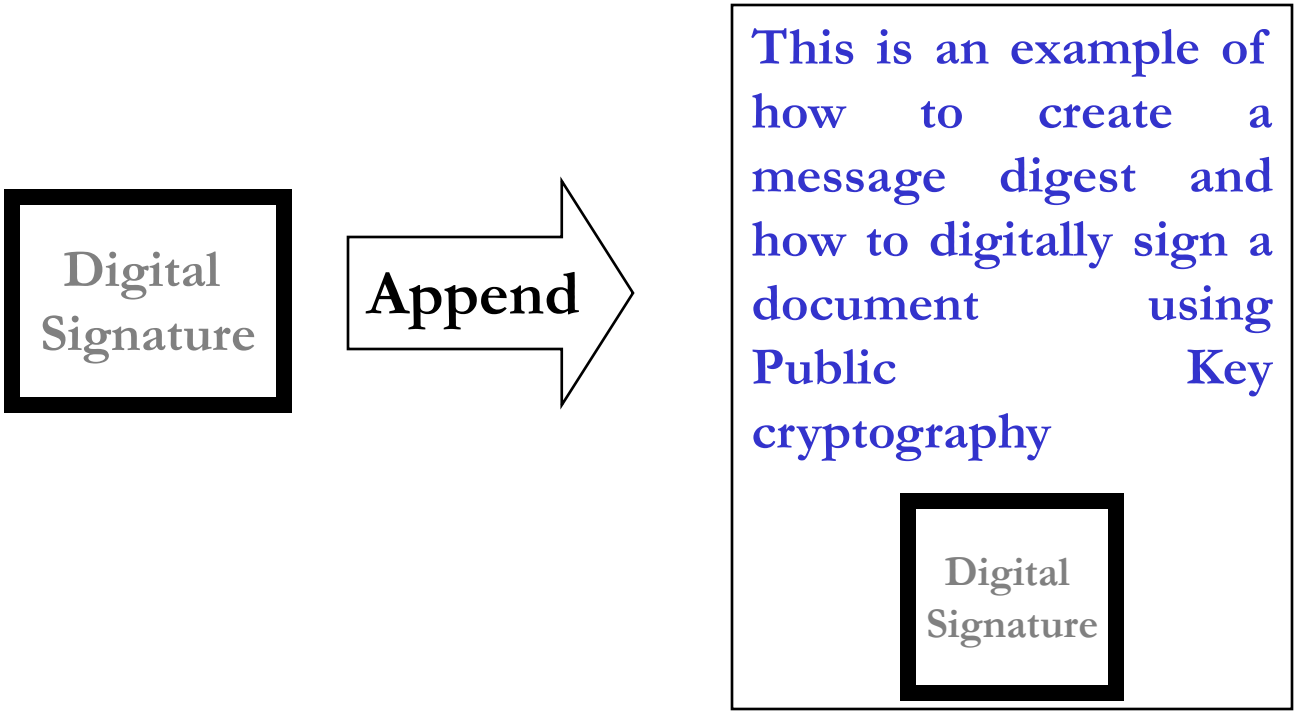
Digital Signing – Step 1

This is an example of how to create a message digest and how to digitally sign a document using Public Key cryptography

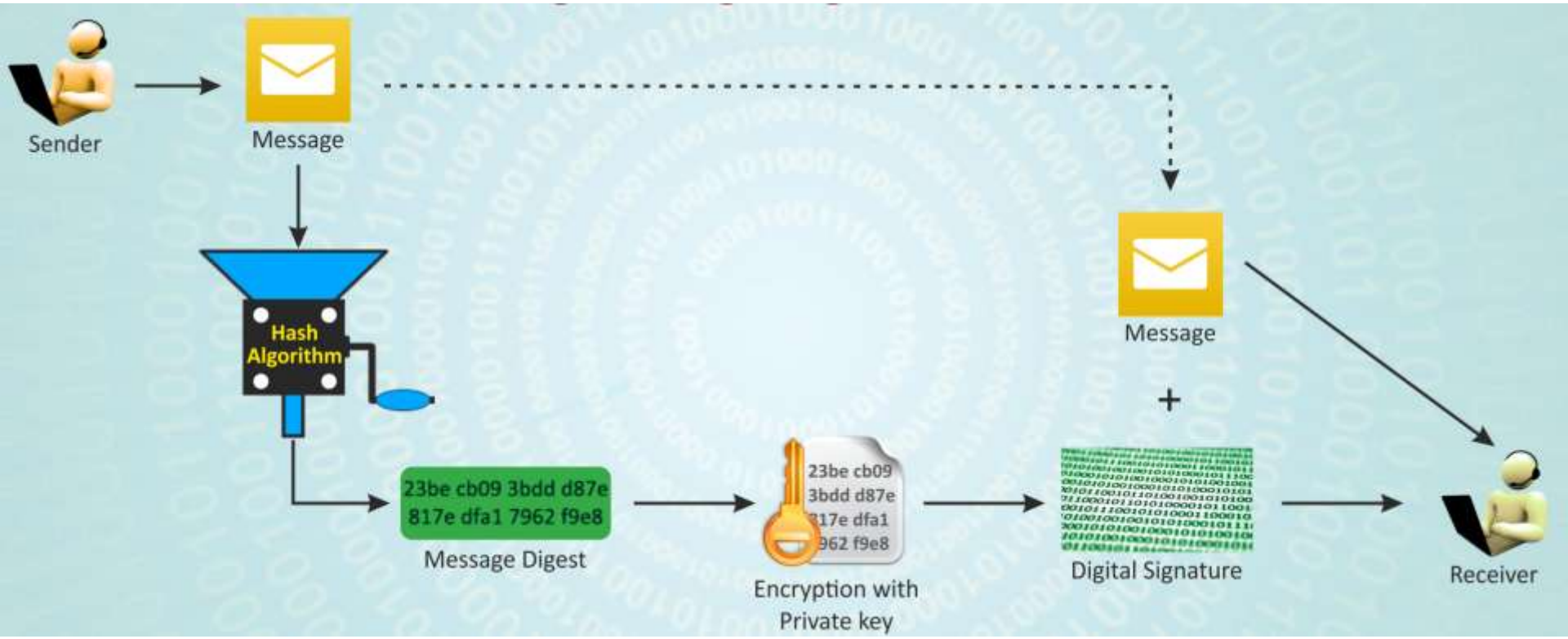


Digital Signing – Step 2

Digital Signing – Step 3



Digital Signing Process



Digital Signature Verification

This is an example of how to create a message digest and how to digitally sign a document using Public Key cryptography

Digital Signature

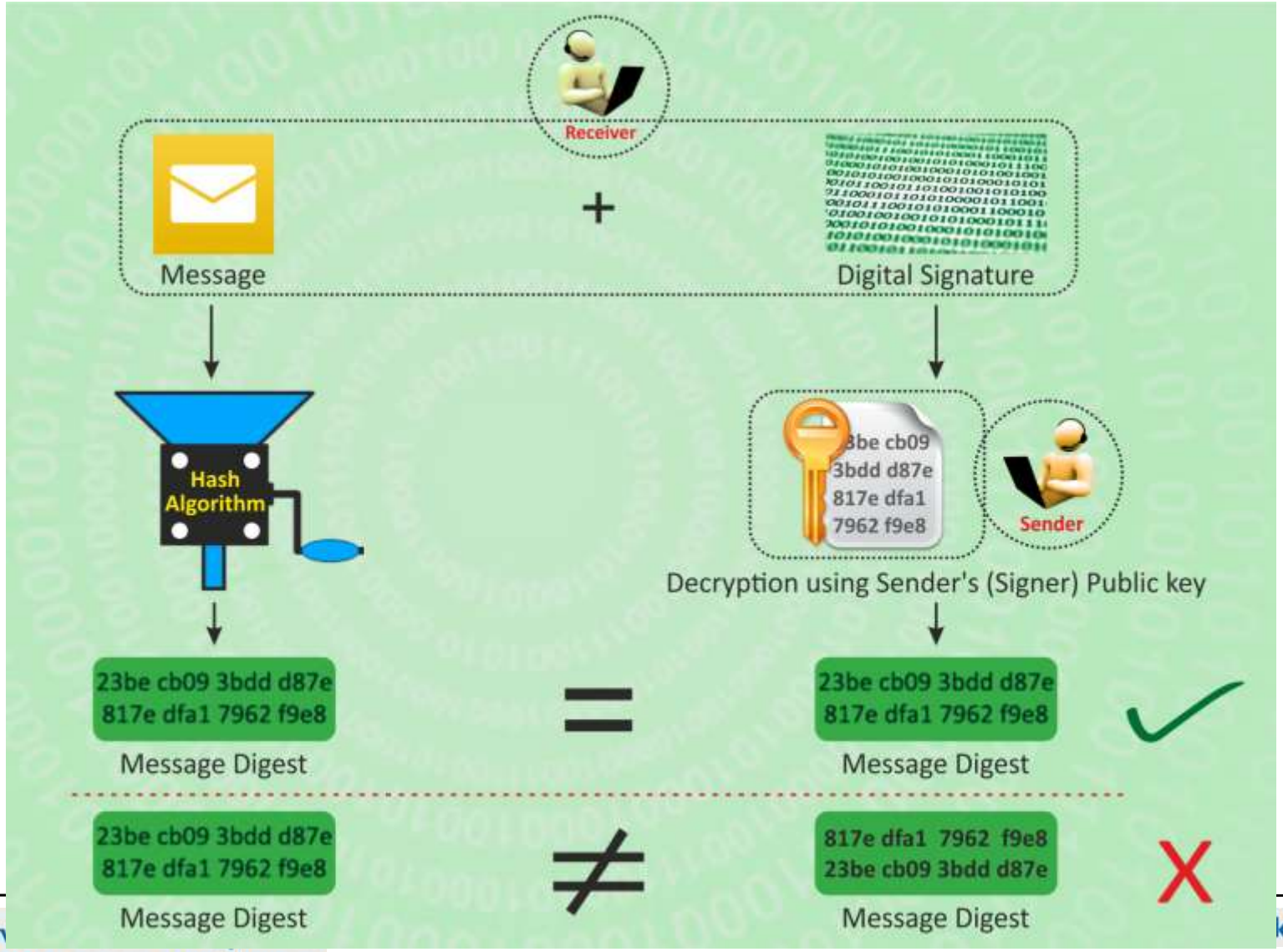
Hash

Message Digest

Decrypt with public key

Message Digest

Digital Signature Verification



General Conventions

- Signing – Private Key of the Signer
- Verification – Public Key of the Signer

Digital Signatures - Examples

I agree

efcc61c1c03db8d8ea8569545c073c814a0ed755

My place of birth is Gwalior.

fe1188eecd44ee23e13c4b6655edc8cd5cdb6f25

I am 62 years old.

0e6d7d56c4520756f59235b6ae981cdb5f9820a0

I am an Engineer.

ea0ae29b3b2c20fc018aaca45c3746a057b893e7

I am a Engineer.

01f1d8abd9c2e6130870842055d97d315dff1ea3

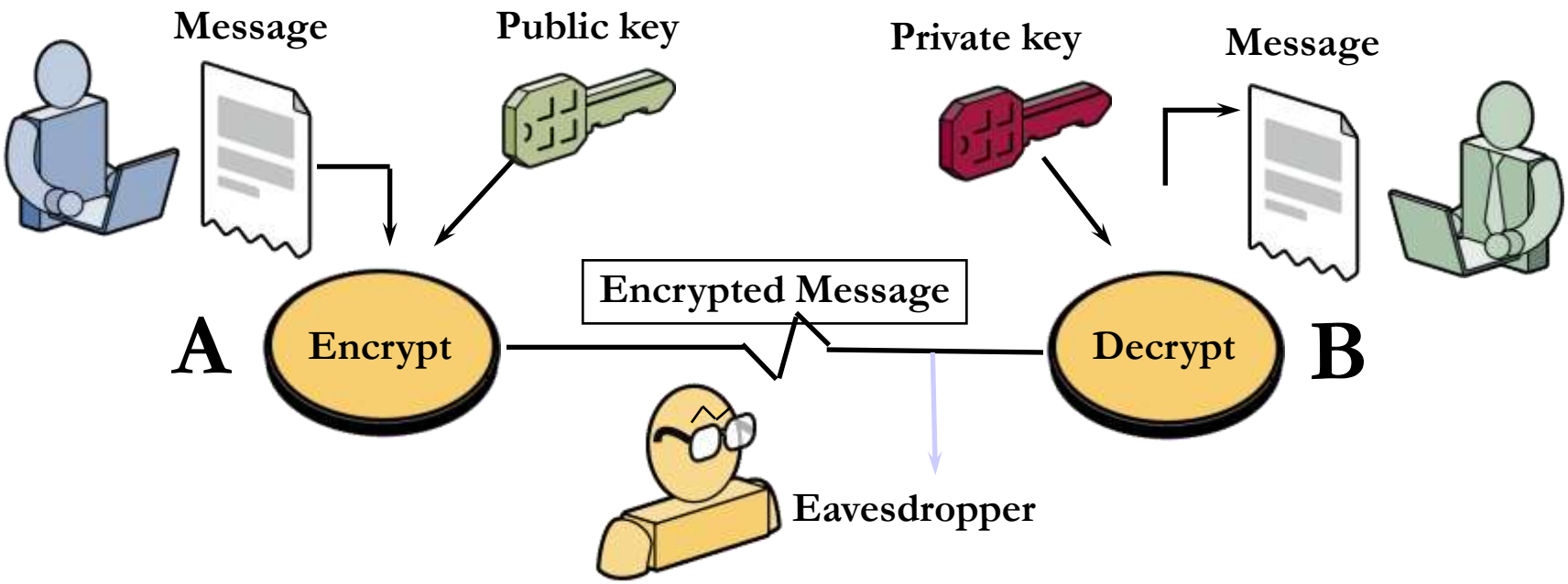
- These are digital signatures of same person on different documents

---

- **Digital Signatures are numbers**
- **They are content and signer dependent**

Achieving Confidentiality

Asymmetric Key Encryption - Confidentiality



General Conventions

- Encryption – Public Key of the Receiver
- Decryption – Private Key of the Receiver

Digital Signature Certificate (DSC)

What is Digital Signature Certificate (DSC)?

DSC is an electronic document used to prove ownership of a public key. The certificate includes

- Information about its owner's identity,
- Information about the key,
- The Digital Signature of an entity that has verified the certificate's contents are correct.

Veeru Info:
Name: Veeru
Department: AMD

Certificate Info:
Serial No: 93 15 H0
Exp Date: dd mm yy

Veeru's Public Key

Sign

Certifying Authority (CA) ?

Certifying Authority (CA)

- Certifying authority is an entity which issues Digital Certificate
- It is a Trusted third party
- CA's are the important characteristics of Public Key Infrastructure (PKI)

Responsibilities of CA

- Verify the credentials of the person requesting for the certificate (RA's responsibility)
- Issue certificates
- Revoke certificate
- Generate and upload CRL

Sample Certificate

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data to be signed with the current time

* Refer to the certification authority's statement for details.

Issued to: Rajendran Balaji

Issued by: NIC sub-CA for NIC 2011

Valid from 2/24/2014 **to** 2/23/2016

You have a private key that corresponds to this certificate.

Issuer Statement

OK

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Serial number	31 11 99 e6 b8 a3 74 47 9e ab
Signature algorithm	sha256RSA
Issuer	NIC sub-CA for NIC 2011, Sub...
Valid from	Monday, February 24, 2014 6...
Valid to	Tuesday, February 23, 2016 6...
Subject	Rajendran Balaji, Karnataka, 5...
Public key	RSA (2048 Bits)
Subject Key Identifier	0c 34 5a 29 d9 86 03 5a 35 19...

```
30 82 01 0a 02 82 01 01 00 94 af f2 4f ca
61 28 fb 13 b2 cb 82 07 c1 37 c1 9a 5e a2
49 6f a2 69 19 78 61 8e 41 c1 e0 48 da 1c
48 af 6a 43 4f c9 36 8b 61 82 e8 e8 61 d2
b3 08 b1 59 38 06 ed af 37 ec 9d 6f a0 50
ec ae 29 38 d8 5c 21 07 40 38 80 a3 e7 bb
ea de 0a 8f f8 55 8f 0a b2 ea 52 b8 c4 d0
1a bb 81 29 82 33 69 77 cf cb 23 e0 f9 8b
1a 7e ff 63 92 8d 6d f3 2d 33 d8 51 0f 39
```

Edit Properties... | Copy to File...

OK

Smart Cards

- The Private key is generated in the crypto module residing in the smart card.
- The key is kept in the memory of the smart card.
- The key is highly secured as it doesn't leave the card, the message digest is sent inside the card for signing, and the signatures leave the card.
- The card gives mobility to the key and signing can be done on any system. (Having smart card reader)

Hardware Tokens

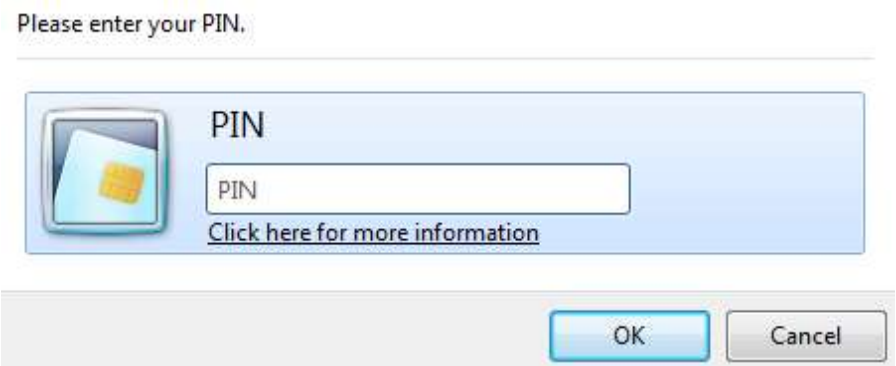
- They are similar to smart cards in functionality as
  - Key is generated inside the token.
  - Key is highly secured as it doesn't leave the token.
  - Highly portable.
  - Machine Independent.

- iKEY is one of the most commonly used token as it doesn't need a special reader and can be connected to the system using USB port.

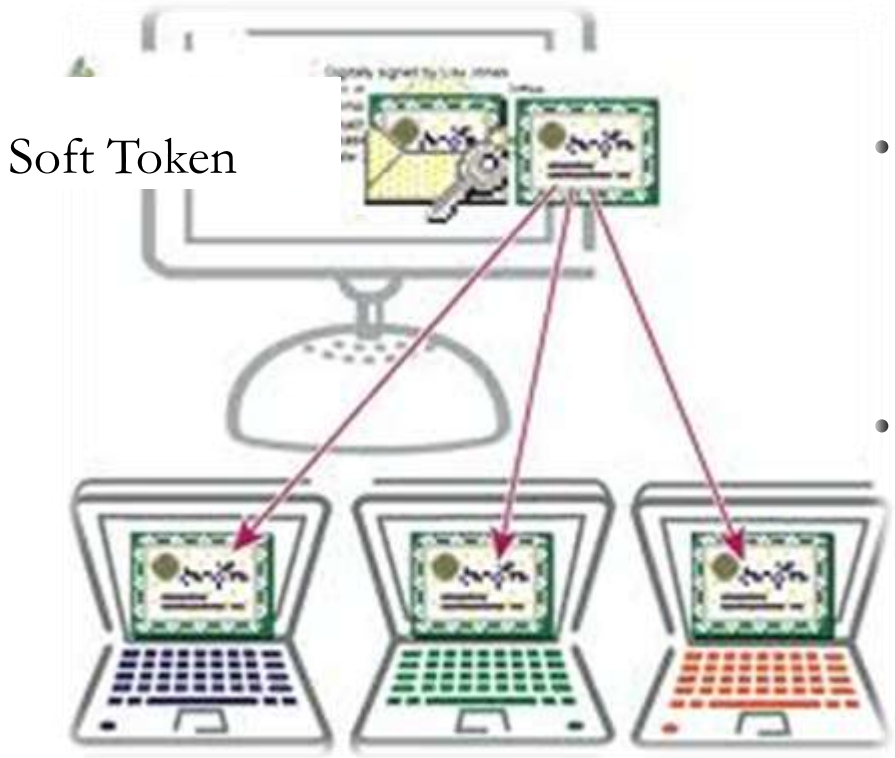
Private key protection

- The Private key generated is to be protected and kept secret. The responsibility of the secrecy of the key lies with the owner.

- The key is secured using
  - PIN Protected Soft token
  - Smart Cards
  - Hardware USB Tokens



PIN protected Soft Tokens



- The Private key is encrypted and kept on the Hard Disk in a file, this file is password protected.
- This forms the lowest level of security in protecting the key, as
  - The key is highly reachable.
  - PIN can be easily known or cracked.
- Soft tokens are not preferred because
  - The key becomes static and machine dependent.
  - The key is in a known file format.

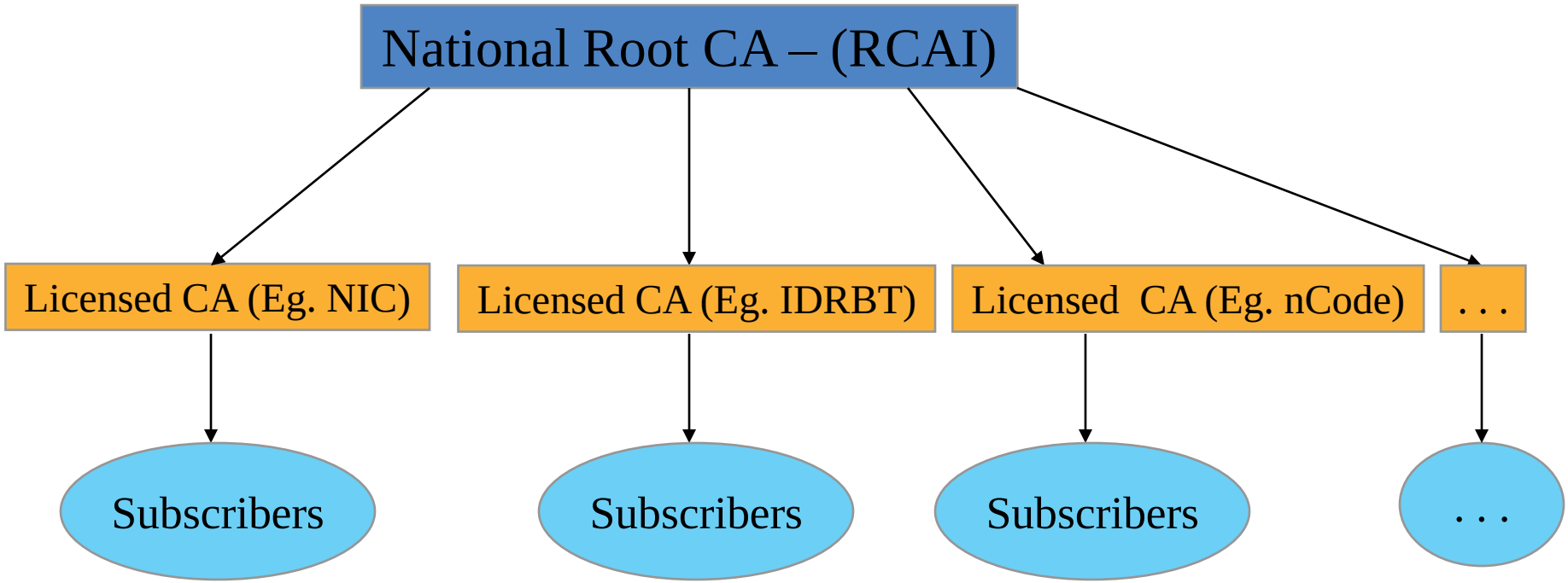
General Security Lessons

- Risks are inherent in any cryptographic system
- PKI is not a one-stop solution for all your security needs
- Any security system is only as safe as the weakest link in a security chain!

Trust Model

Hierarchical Trust Model

- For a Digital Signature to have legal validity, it must derive its trust from the Root CA certificate

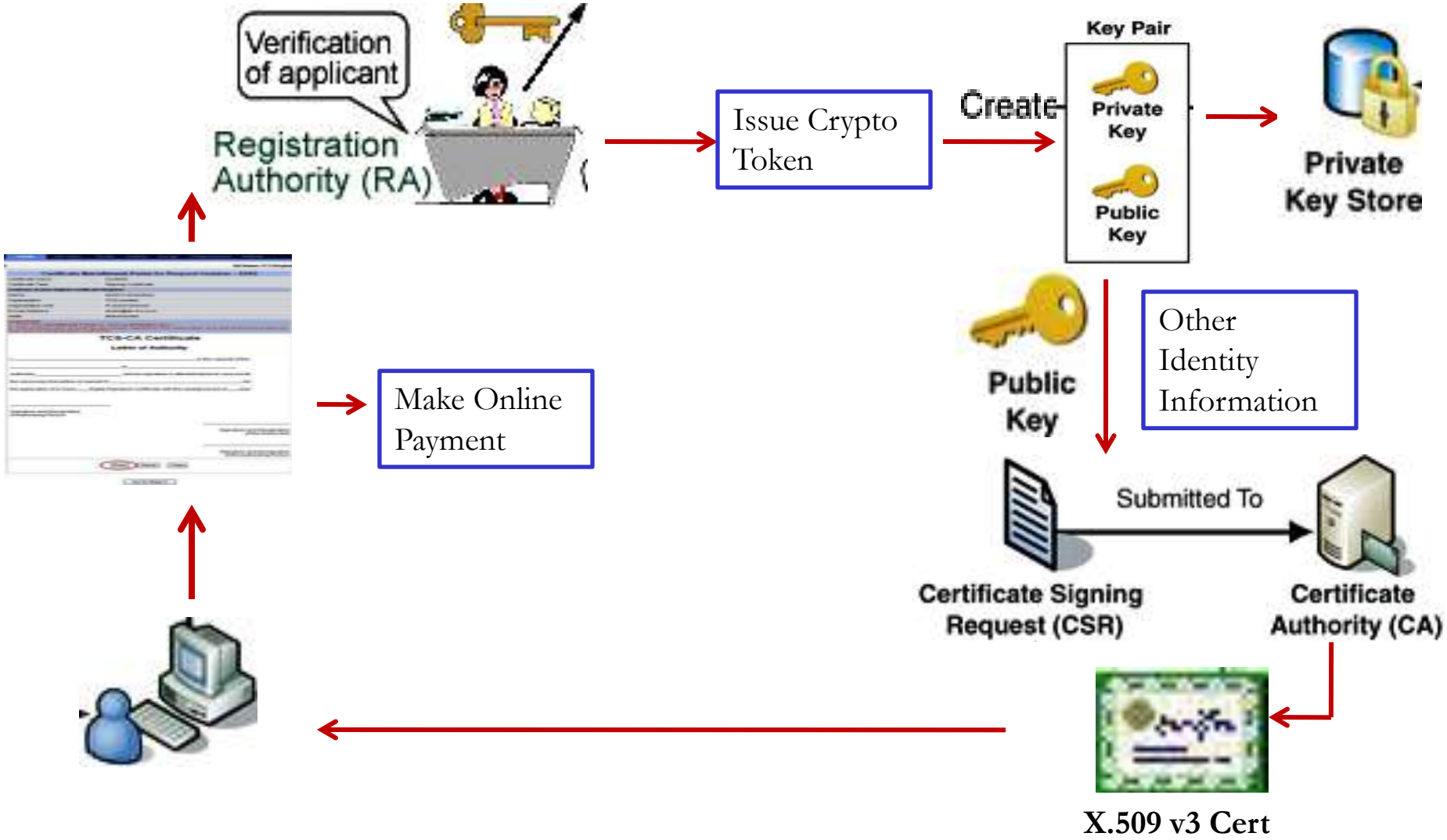


Licensed CA's in India

- National Root CA (RCAI) – operated by CCA
  - Only issues CA certificates for licensed Cas
- 8 CAs licensed under the National Root CA
  - National Informatics Centre (https://nicca.nic.in)
  - eMudhra (www.e-mudhra.com)
  - TCS (www.tcs-ca.tcs.co.in)
  - nCode Solutions CA(www.ncodesolutions.com)
  - SafeScrypt (www.safescrypt.com)
  - IDRBT CA (www.idbrtca.org.in)
  - MTNL
  - Customs and Central Excise
- As of April2015, approx. 8 Million DSCs have been issued

Certificate Issuance Process

Certificate Issuance Process



Types of Certificates

Types of Certificates

- Signing Certificate
  - Issued to a person for signing of electronic documents
- Encryption Certificate
  - Issued to a person for the purpose of Encryption;
- SSL Certificate
  - Issued to a Internet domain name (Web Servers, Email Servers etc…)

Certificate Classes

Classes of Certificates

- 3 Classes of Certificates
  - Class – 1 Certificate
    - Issued to Individuals
    - Assurance Level: **Certificate will confirm User's name and Email address**
    - Suggested Usage: **Signing certificate** primarily be used for signing personal emails and **encryption certificate** is to be used for encrypting digital emails and **SSL certificate** to establish secure communication through SSL

Classes of Certificates

- Class – 2 Certificate
  - Issued for both business personnel and private individuals use
  - Assurance Level: **Conforms the details submitted in the form including photograph and documentary proof**
  - Suggested Usage: **Signing certificate** may also be used for digital signing, code signing, authentication for VPN client, Web form signing, user authentication, Smart Card Logon, Single sign-on and signing involved in e-procurement / e-governance applications, in addition to Class-I usage

Classes of Certificates

– Class – 3 Certificate

- Issued to Individuals and Organizations
- Assurance Level: **Highest level of Assurance; Proves existence of name of the organization, and assures applicant's identity authorized to act on behalf of the organization.**
- Suggested Usage: **Signing certificate** may also be used for digital signing for discharging his/her duties as per official designation and also **encryption certificate** may also be used for encryption requirement as per his/her official capacity

Certificate Lifecycle Management

- A Digital Signature Certificate cannot be used for ever!
- Typical Life cycle scenario of Digital Certificates
  - Use until renewal
    - Certificates are to be reissued regularly on expiry of validity (typically 2 years)
  - Use until re-keying
    - If keys had to be changed
  - Use until revocation
    - If Certificate was revoked, typically when keys are compromised or CA discovers that certificate was issued improperly based on false documents

CRL – Certification Revocation List

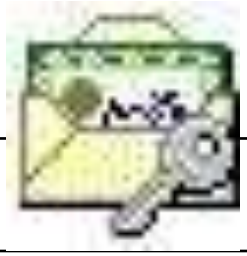
- A list containing the serial number of those certificates that have been revoked
- Why they have been revoked?
  - If keys are compromised and users reports to the CA
  - If CA discovers, false information being used to obtain the certificate
- Who maintains CRLs ?
  - Typically the CA's maintain the CRL

CRL – Certification Revocation List

- How frequently the CRL is updated ?
  - Generally twice a day; based on CA's policies
- Is there any automated system in place for accessing the CRL?
  - OCSP

Certificate Extensions

File Formats with Extensions	Description
.CER	Contains only Public Key
.CRT	Contains only Public Key
.DER	Contains only Public Key
.P12	Contains Public and Private Key
.PFX	Contains Public and Private Key
.PEM, .KEY, .JKS	Contains Public and Private Key
.CSR	Certificate Signing Request
.CRL	Certificate Revocation List



Legal aspects of Digital Signature as per Indian IT Act

Objective of the Indian IT Act 2000

- To grant legal recognition to records maintained in electronic form
- To prescribe methods for authenticating electronic records
- To establish a hierarchical trust model with a root CA at the top - CCA to regulate the CAs
- To define computer system and computer network misuse and make it legally actionable

IT Act 2000

- IT Act 2000 made changes in the Law of Evidence, and provides
  - Legal recognition for electronic records and electronic signatures, which paves the way for
    - Legal recognition for transactions carried out by electronic communication
    - Acceptance of electronic filing of documents with the government agencies
    - Changes in the IPC and the Indian Evidence Act 1872 were made accordingly
    - IT Act 2000 has extra-territorial jurisdiction to cover any offense or contravention committed outside India

Authentication Method Prescribed by the Indian IT Act 2000

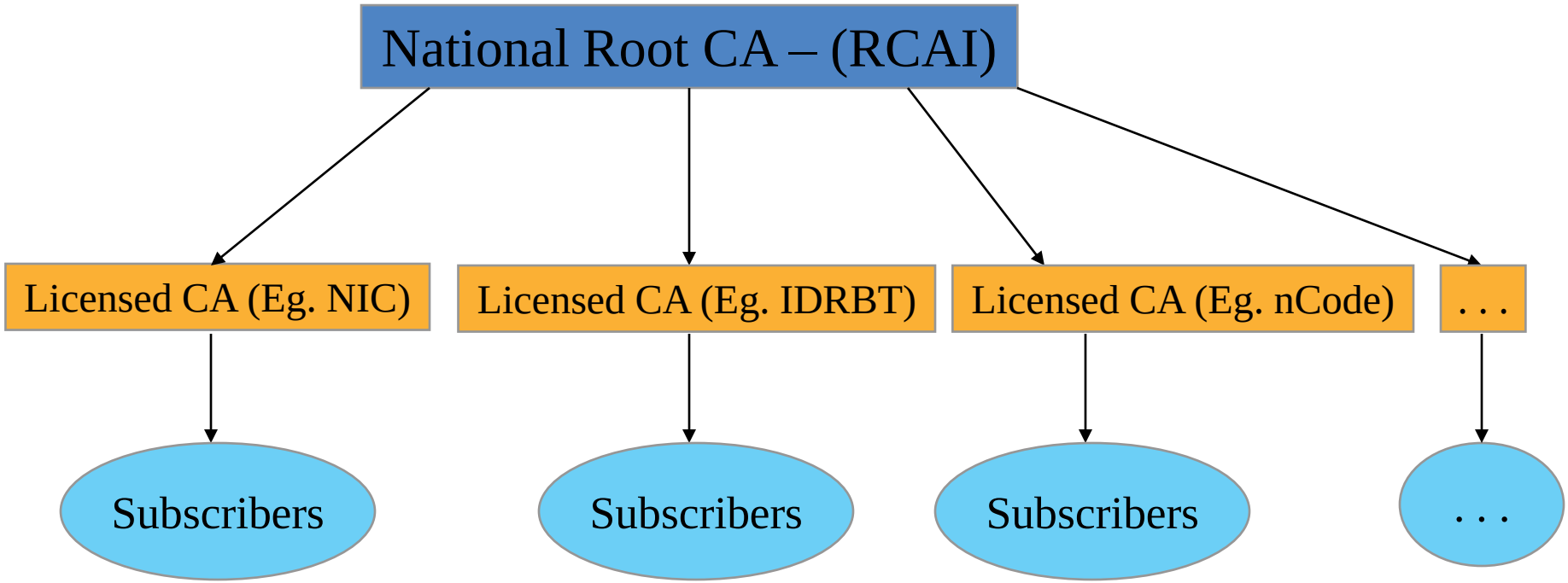
- The Act specifies that authentication must be by Digital Signatures based upon *Asymmetric Key Cryptography* and *Hash Functions*.
  - The National Root CA uses a 2048 bit RSA key pair
  - Other CA and end entities use 2048 bit RSA key pairs

Regulation of Certifying Authorities

- The IT act mandates a hierarchical Trust Model
- The IT Act provides the Controller for Certifying Authorities (CCA) to license and regulate the working of CA.
- The CCA operates RCAI for certifying (signing) the public keys of CA's using it private key

Hierarchical Trust Model

- For a Digital Signature to have legal validity, it must derive its trust from the Root CA certificate



IT Act 2000 on CCA and CAs

- Under the Indian Law, section 35 of the IT (Amendment) Act, 2008 deals with certification and certifying authorities
- IT Act 2000 recognizes even foreign CAs and gives the power to the CCA to decide on the same
  - CCA can also revoke the certificate for violation in any restriction or condition on which it was recognized by giving reasons in writing.

Present Digital Signature & PKI Implementations in India

PKI enabled Applications

1	**e-Invoice**	**(B2C)**
2	**e-Tax Filing**	**(G2C)**
3	**e-Customs**	**(G2B)**
4	**e-Passport**	**(G2C) -** Presently in India, the Ministry of External Affairs has started issuing e-Passports in Karnataka state with the fingerprints and the digital photo of applicant
5	**e-Governance**	**Bhoomi (G2C)** a PKI enabled registration and Land Records Services offered by Govt. of Karnataka to the people. All the land records and certificates issued are digitally signed by the respective officer
6	**e-Payment**	**(B2B) -** In India, currently between banks fund transfers are done using PKI enabled applications whereas between customers and vendors such as online shopping vendor the payment is done through SSL thereby requiring the vendor to hold DSC)

PKI enabled Applications

7	**e-Billing**	**(B2C)** -The electronic delivery and presentation of financial statement, bills, invoices, and related information sent by a company to its customers)
8	**e-Procurement**	**G2B , B2B**
9	**e-Insurance Service**	**(B2C) -** Presently the users are getting the E-Premium Receipts etc. which is digitally signed by the provider

C-DAC Activities in PKI Domain

- PKI Knowledge Dissemination Program
  - An effort to spread awareness and build competencies in the domain across the country
- PKI Body of Knowledge
  - To develop a BoK with inputs from various sections of users
    - Researchers – Algorithms and new directions in PKI
    - Developers – PKI Administration and implementation issues
    - Policy Makers - Laws
    - End Users and Applications

Summary

- PKI is an ecosystem comprising of Technology, Policy and Implementations
  - Digital Signatures provide **A**uthenticity, **I**ntegrity, and **N**on-Repudiation for electronic documents & transactions
  - Asymmetric Key system enables **C**onfidentiality
- General Conventions
  - Signing – Private Key of the Signer
  - Verification – Public Key of the Signer
  - Encryption – Public Key of the Receiver
  - Decryption – Private Key of the Receiver

References

- Cryptography and Network security – Principles and Practice by William Stallings
- Applied Cryptography: Protocols, Algorithms, and Source Code in C by Bruce Schneier
- Handbook of Applied Cryptography, by Alfred Menezes and Paul Van Oorschot
- Ryder, Rodney D, Guide to Cyber Laws, 3rd Edition, Wadhwa & Company, New Delhi
- Digital Certificates: What are they?: http://campustechnology.com/articles/39190_2
- Digital Signature & Encryption: http://www.productivity501.com/digital-signatures-encryption/4710/
- FAQ on Digital Signatures and PKI in India - http://www.cca.gov.in/cca/?q=faq-page
- Controller of Certifying Authorities – www.cca.gov.in
- More Web Resources
  - For events, slides and Discussions: www.seekha.in/event/pki
  - Social Media:

www.facebook.com/pkiindia @pkiindia

Thank You

pki@cdac.in