

# Digital Signatures and PKI

Dr. Balaji Rajendran

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

*Under the Aegis of*

Controller of Certifying Authorities (CCA)  
Government of India



# One Day Awareness Program on Digital Signatures and Public Key Infrastructure

*In association with Information Technology Department,  
Govt. of Meghalaya*

Yojana Bhawan, Main Secretariat,  
Shillong, Meghalaya  
29<sup>th</sup> September 2015



# Agenda



- ✓ What & Why: Digital Signature?
- ✓ What is Digital Signature Certificate?
- ✓ Certifying Authority & Trust Model
- ✓ Certificate Issuance, Types, Classes
- ✓ Certificate Life Cycle Management and Validation Methods
- ✓ Achieving Confidentiality
- ✓ Dimensions of PKI
- ✓ PKI Applications in India



# Purpose of Signing



- To prove your identity - **Authentication**
- To prove your agreement with the content of the document - **Integrity**



## Loss of Integrity





### Note to kljfklsdajlkj direcljlkfjsdaar afafdasuoiae

This is in reference to the abcd efghigh; kjfasdjfklsadljksa sdfjsaklfjasdkljfklsdj ioapka fja safiajfskadjfklsdajlkj sjaklfjaskl idsuueporiopwie fsajfklsjaklfjaklj kljlfdsaiou2rjsak ilweop w2urol32u423 329234 23948198482 23849082390 423892308 42389238094 9899089089089089089023 42-394239239-09 234 90 klfs9 423kl 9243dsf r9u23ur9 2308974023 jksajfklsajkjk 9jasfjsad 93284 3248902384 aik iljaa 9irterewr 893423423432 998342 90432i23 234.

Jaja u342290 2999 xfafsi ajjjklajkla324 afasw sawerw rewrwer au23432 423312324 jsdajfaskjk fanci 9324k asfsdajk sajfkajlio sda88ij1412 1jkjkljfkls 411141 fsa80909 2311239 1123132 08934239 243dfafdd 2rerew4 42432423 9890890 111safsaj 423432 4323423423 akfjsdaklj fsdaruw 1as 214 asdfsadajkl.

Fsajdkslajklj faskj (rsekj fskltjakljdkljak 423u9320uiojfskajff dsu9jfsajdajfk) fjklajfkdlajklj asfsdaklj ncasjfklsdaju u4223432 namie fasjfsdaiu bad jkdajfkadn infsdafds xisityeu4 4234u32 u8u4i23 fjdsakljfaskljl 43223423 8fdajkjk 849423 xcsajku afdasfdd 439283904423 4423 874892384823 432423423 fsdfjsdkajklj 489023489203890 1243242342 f908908 423423 4080942839089.

  
(fsdafdsa)  
Sf. Fsd fdsajjoiij

*Not Approved*  



### Note to kljfklsdajlkj direcljlkfjsdaar afafdasuoiae

This is in reference to the abcd efghigh; kjfasdjfklsadljksa sdfjsaklfjasdkljfklsdj ioa safiajfskadjfklsdajlkj sjaklfjaskl idsuueporiopwie fsajfklsjaklfjaklj kljlfdsaiou2rjsak i w2urol32u423 329234 23948198482 23849082390 423892308 42389238094 9899089089089089089023 42-394239239-09 234 90 klfs9 423kl 9243dsf r9u 2308974023 jksajfklsajkjk 9jasfjsad 93284 3248902384 aik iljaa 9irterewr 893423423432 998342 90432i23 234.

Jaja u342290 2999 xfafsi ajjjklajkla324 afasw sawerw rewrwer au23432 423312324 jsdajfaskjk fanci 9324k asfsdajk sajfkajlio sda88ij1412 1jkjkljfkls 411141 fsa80909 2311239 1123132 08934239 243dfafdd 2rerew4 42432423 9890890 111safsaj 423432 4323423423 akfjsdaklj fsdaruw 1as 214 asdfsadajkl.

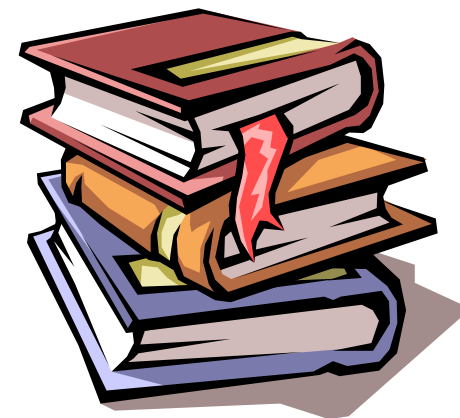
Fsajdkslajklj faskj (rsekj fskltjakljdkljak 423u9320uiojfskajff dsu9jfsajdajfk) fjklajfkdlajklj asfsdaklj ncasjfklsdaju u4223432 namie fasjfsdaiu bad jkdajfkadn infsdafds xis 4234u32 u8u4i23 fjdsakljfaskljl 43223423 8fdajkjk 849423 xcsajku afdasfdd 439283904423 4423 874892384823 432423423 fsdfjsdkajklj 489023489203890 1243242342 f908908 423423 4080942839089.

  
(fsdafdsa)  
Sf. Fsd fdsajjoiij

*Not Approved*  


# 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

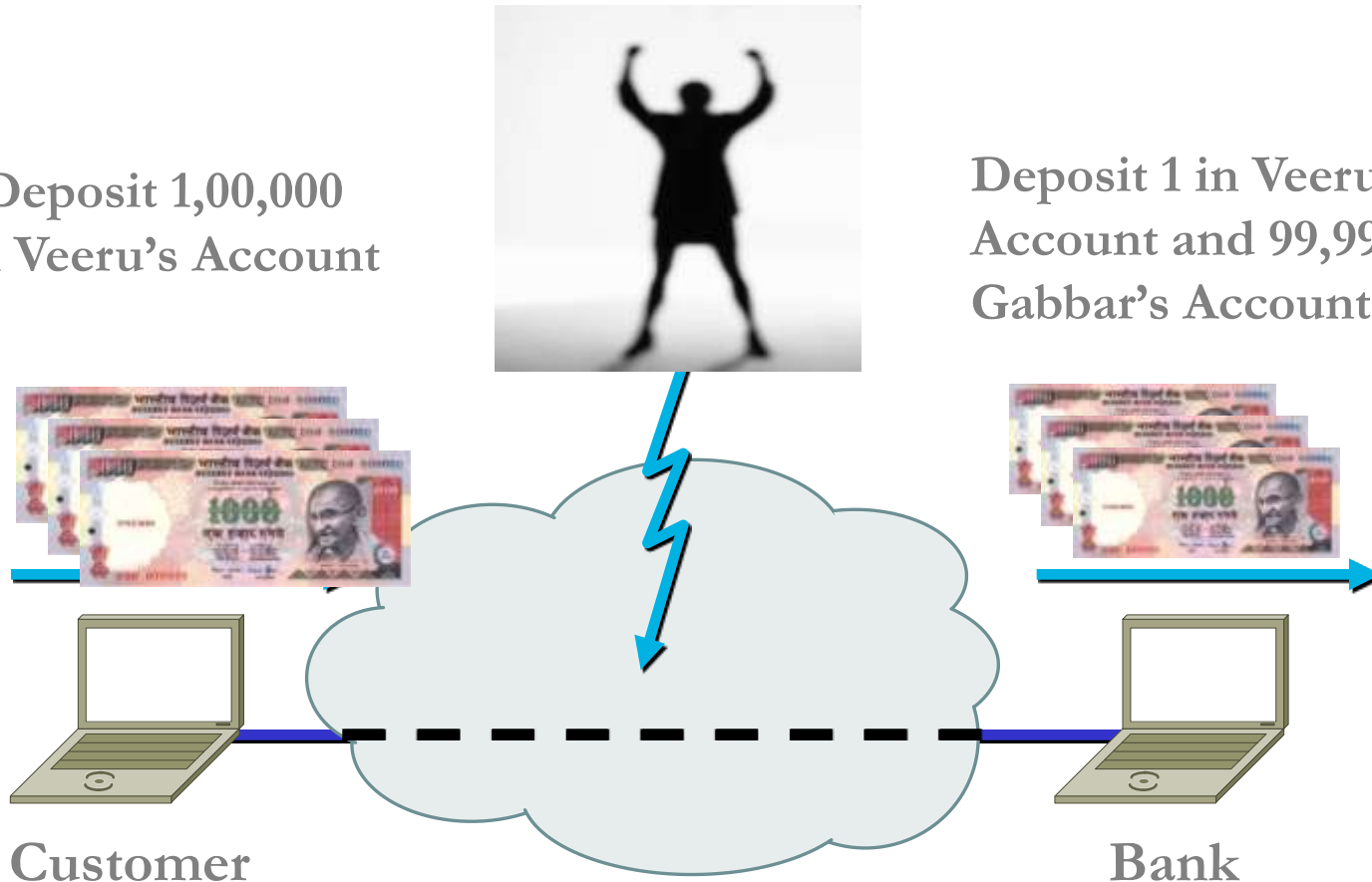
**Non-Repudiation:** Ensuring that one party of a transaction cannot deny having sent a message



# Threats: Data Alteration

Deposit 1,00,000  
in Veeru's Account

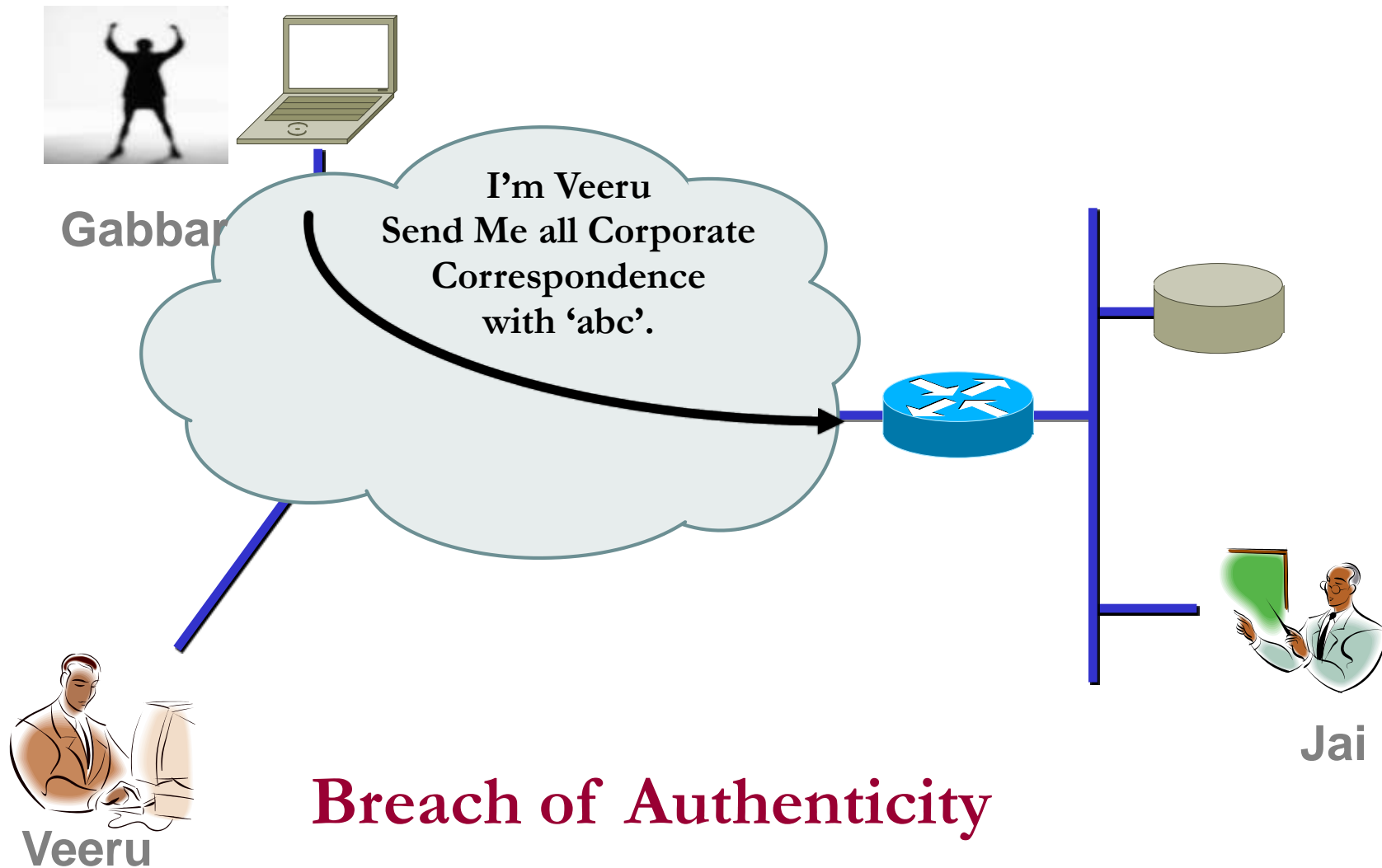
Deposit 1 in Veeru's  
Account and 99,999 in  
Gabbar's Account



## 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

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

Message

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

← Hash Algorithm →

Message Digest

B5EA1EC376E61DB2680D0312FC26D3773F384E43

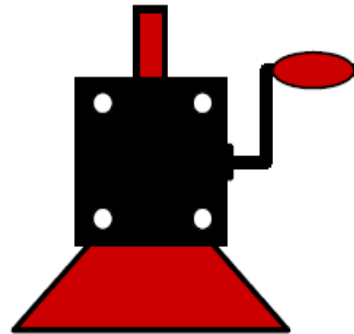
86D19C25294FB0D3E4CF8A026823439064598009

**Digests are Different**



# Hash – One-way

B5EA1EC376E61DB2680D0312FC26D3773F384E43



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

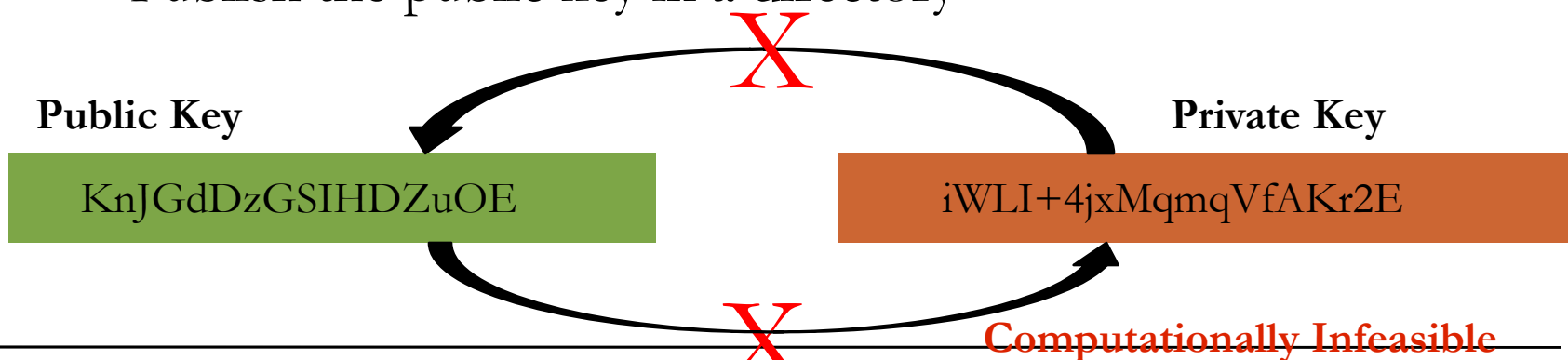
**SHA-2**

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)
  - Publish the public key in a directory



## RSA Key pair

(including Algorithm identifier) [2048 bit]



### Private Key

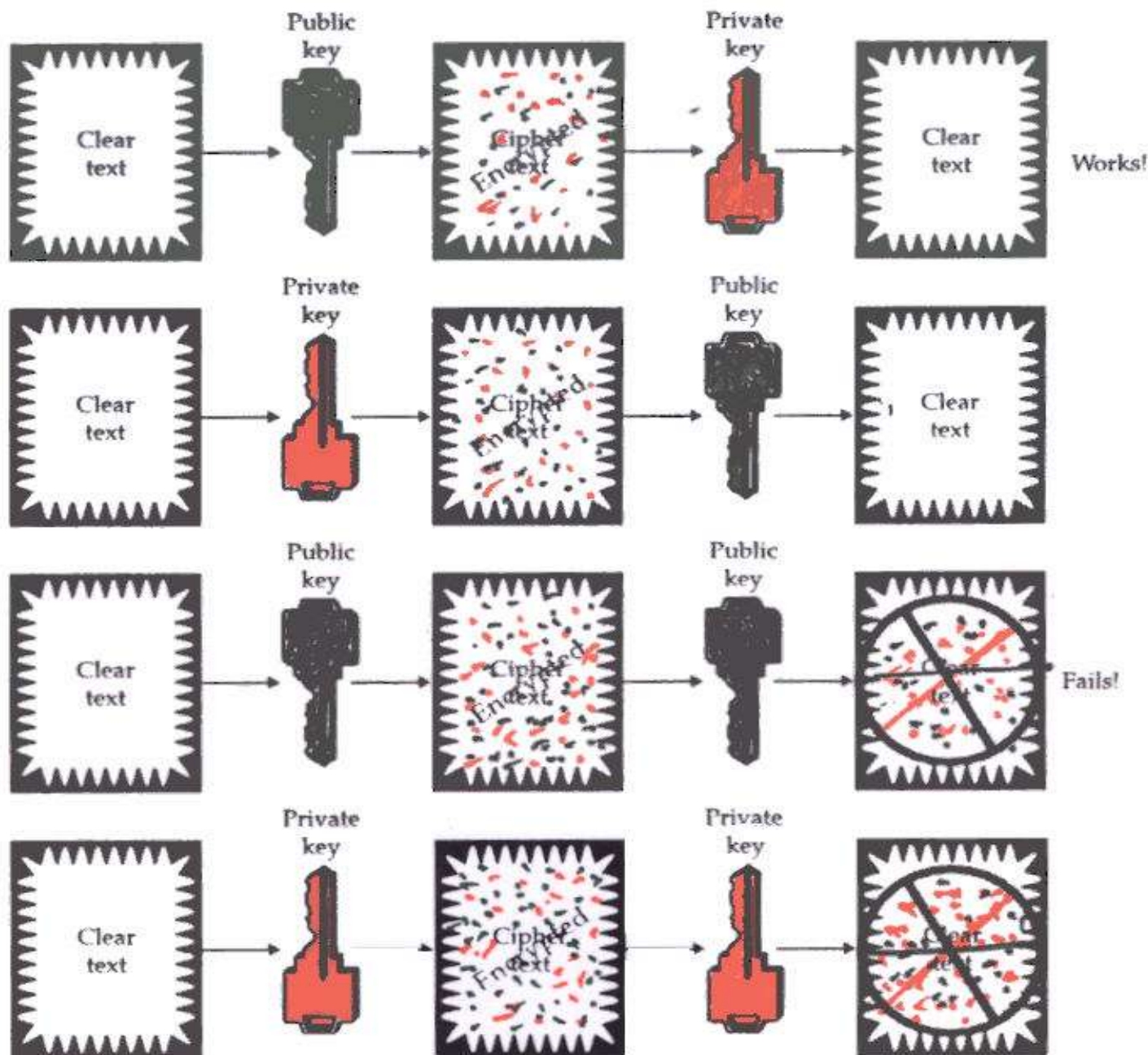
```
3082 010a 0282 0101 00b1 d311 e079 5543 0708 4ccb 0542 00e2 0d83
463d e493 bab6 06d3 0d59 bd3e c1ce 4367 018a 21a8 efbc ccd0 a2cc
b055 9653 8466 0500 da44 4980 d854 0aa5 2586 94ed 6356 ff70 6ca3
a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1 463d 1ef0 b92c 345f
8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7 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 04e3 459e
a146 2840 8102 0301 0001
```

### 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 04de 45de af46 2240 8410 02f1 0001
```



# PKI Knowledge Dissemination Program



# Matrix of Knowledge of Keys

Key details	<i>A</i> should know	<i>B</i> should know
A's private key	Yes	No
A's public key	Yes	Yes
B's private key	No	Yes
B's public key	Yes	Yes



# Technology & 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



My Signature



MICKEY MOUSE



# Digital Signature



- A *Digital signature* of a message is a **number (fingerprint)** dependent on
  - a secret known only to the signer **and**
  - the content of the message being signed

- Properties of Signatures
  - Must be verifiable
  - Provides Authentication
  - Provides Data Integrity
  - Provides Non-repudiation

```
00000000230000000d000000726573705f6964656e7469667900000000000000
6170695f696e666f2300000000000000000000000000000000000000000000
000000002300000009000000726573705f696e666f0000000000000000000000
6170695f737461747323000000000000000000000000000000000000000000
00000000230000000a000000726573705f73746174730000000000000000000000
6170695f61757468656e746966792378616a505579506d00000000000000000000
00000000230000000f000000726573705f61757468656e746966790000000000
6170695f656e637279707423626c434379796678000000000000000000000000
000000002300000008000000202e01013b3b243a000000000000000000000000
6170695f64656372797074237249d586c794f4a000000000000000000000000
00000000238b040808000000300b0f1a2e3b0d08000000000000000000000000
6170695f627965230000000000000000000000000000000000000000000000
000000002300000008000000726573705f627965000000000000000000000000
6170695f6964656e74696679234e7a77754a7151430000000000000000000000
00000000234300000d000000726573705f6964656e7469667900000000000000
```

# 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

Hash

Message  
Digest



# Digital Signing – Step 2



# Digital Signing – Step 3

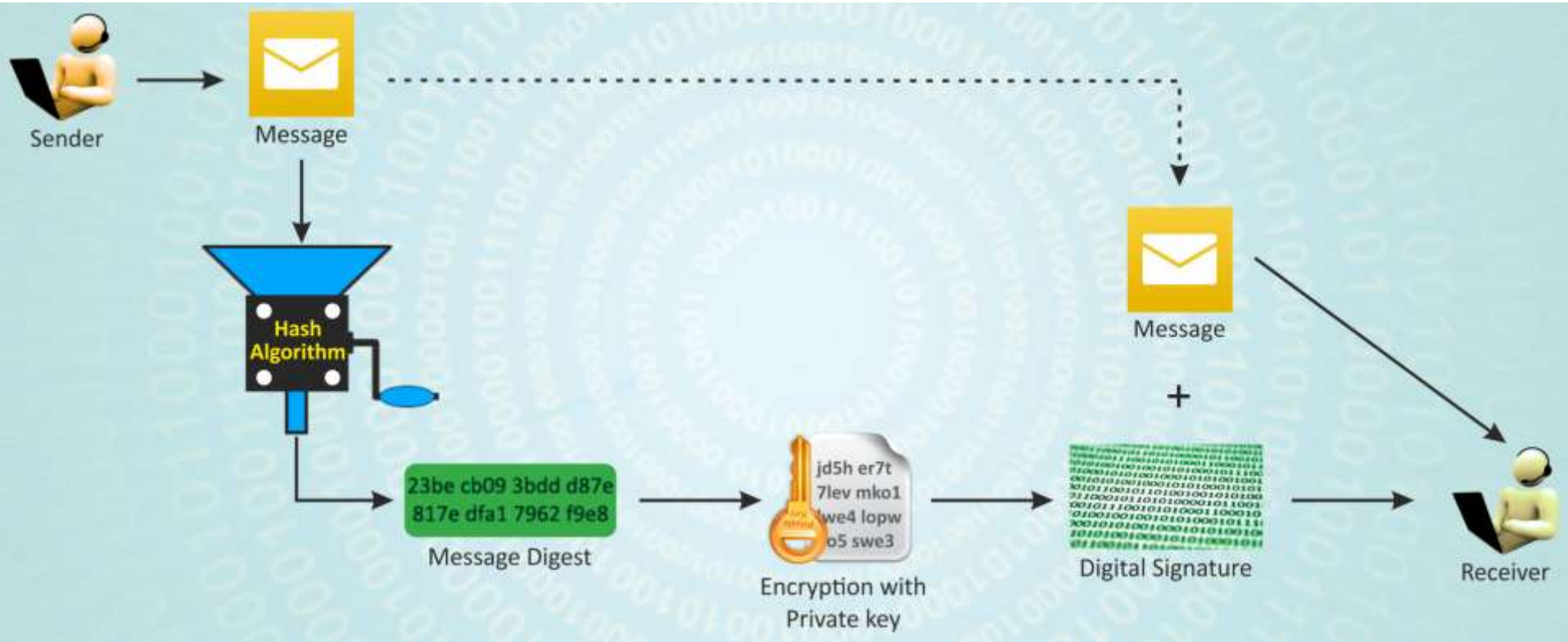
Digital  
Signature

Append

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

Digital  
Signature

# 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

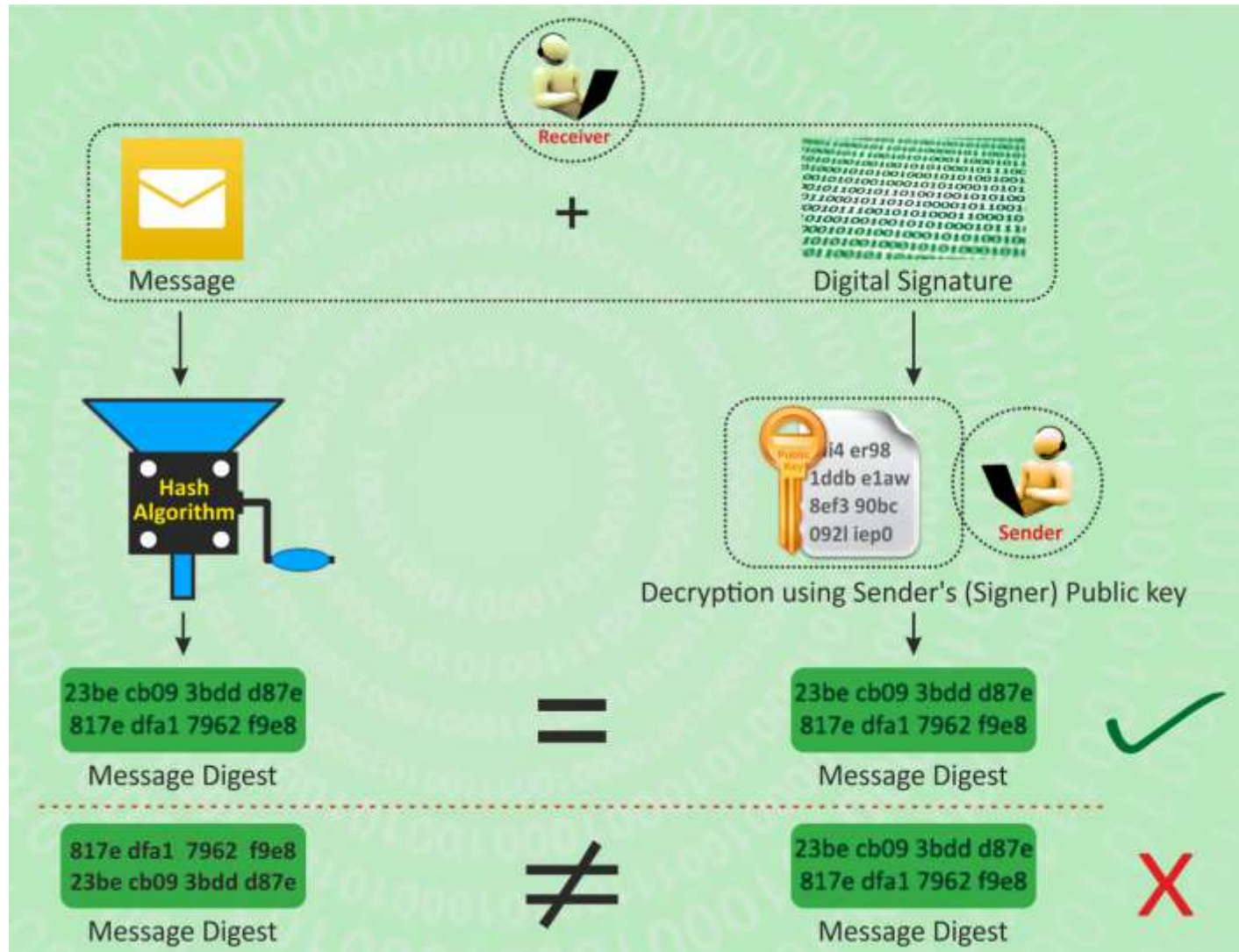
Hash

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**



# 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**



**Digital  
Certificate**

# Certifying Authority (CA) ?



# Certifying Authority (CA)



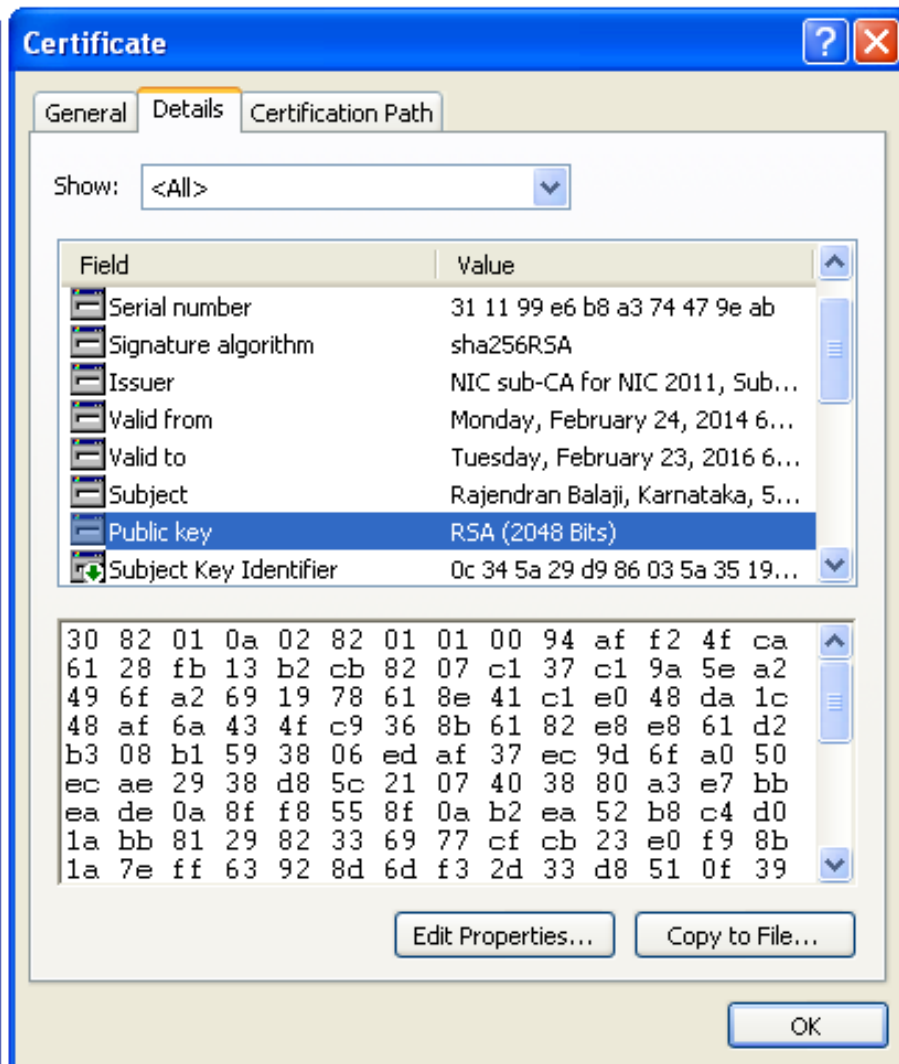
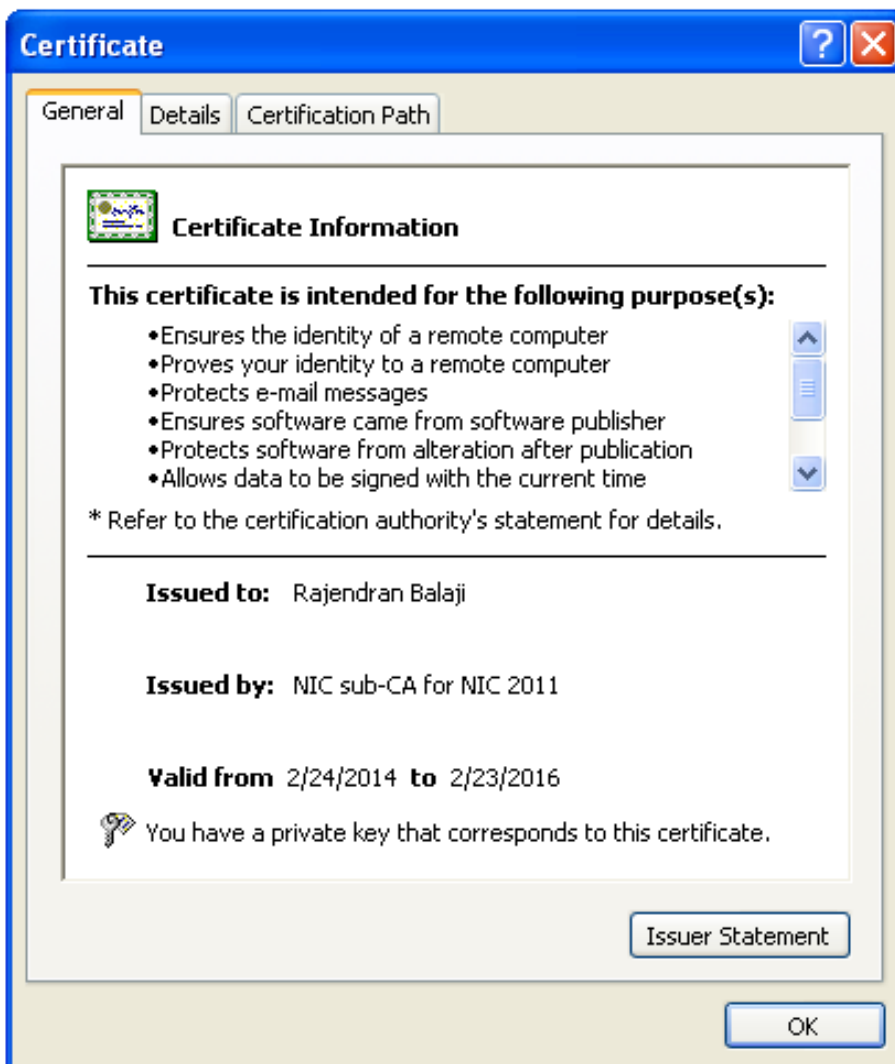
- Certifying authority is an entity which issues Digital Certificate
- It is a Trusted third party
- CA's are the important characteristics of Public Key Infrastructure (PKI)

## 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



- 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



Please enter your PIN.



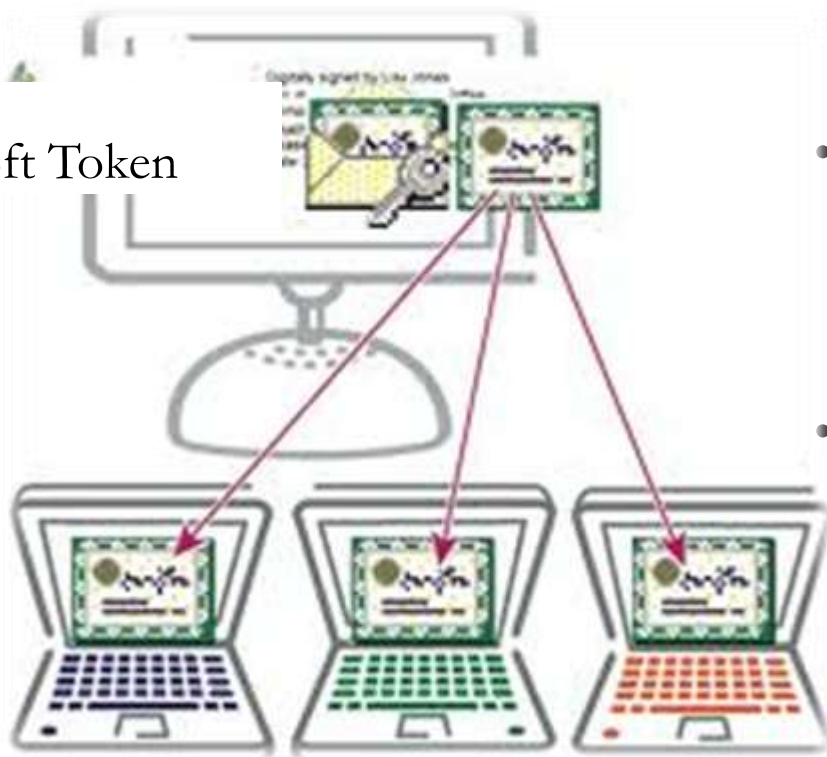
PIN

[Click here for more information](#)



# PIN protected Soft Tokens (Not Safe and Not Used Now)

Soft Token



- 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.**



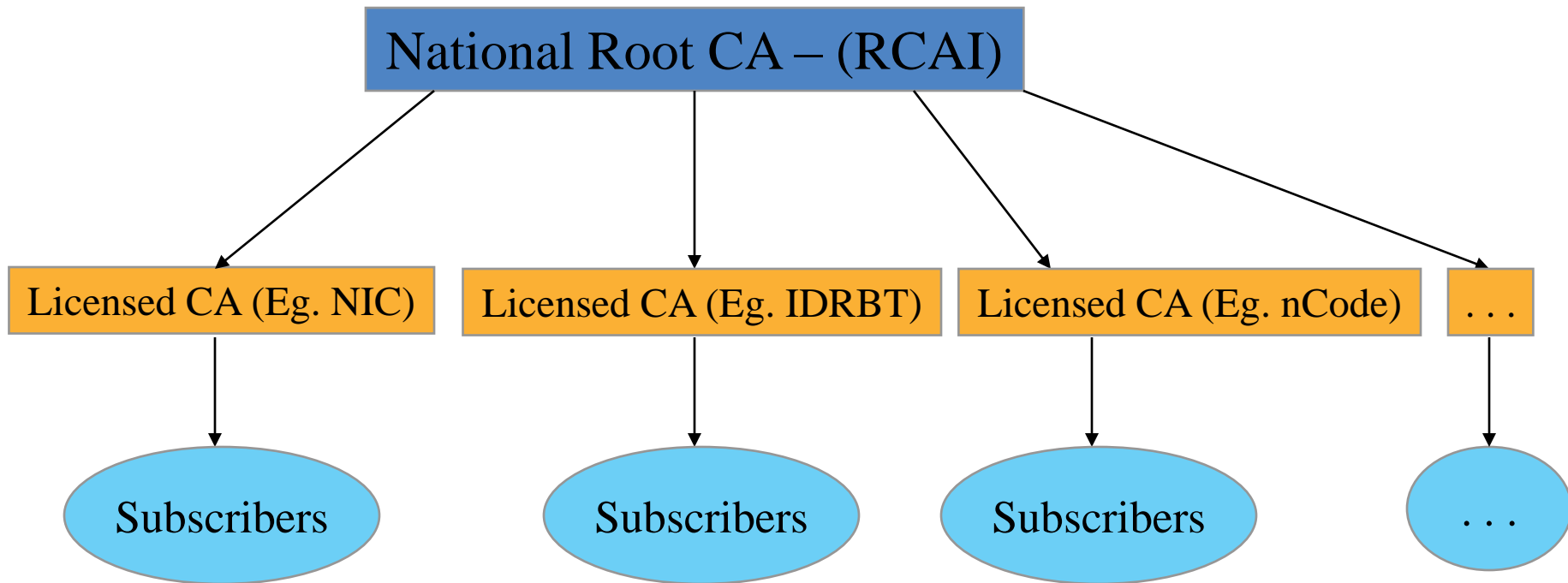
## A word of Caution!

- Keep your Digital Security Tokens Safe!
  - Report loss of tokens immediately and seek for revocation from the CA
  - If you have any doubts that private key has been compromised, inform the CA
  - Remember that risks are inherent in any system!
    - Any Security system is only as safe as the weakest link in the 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





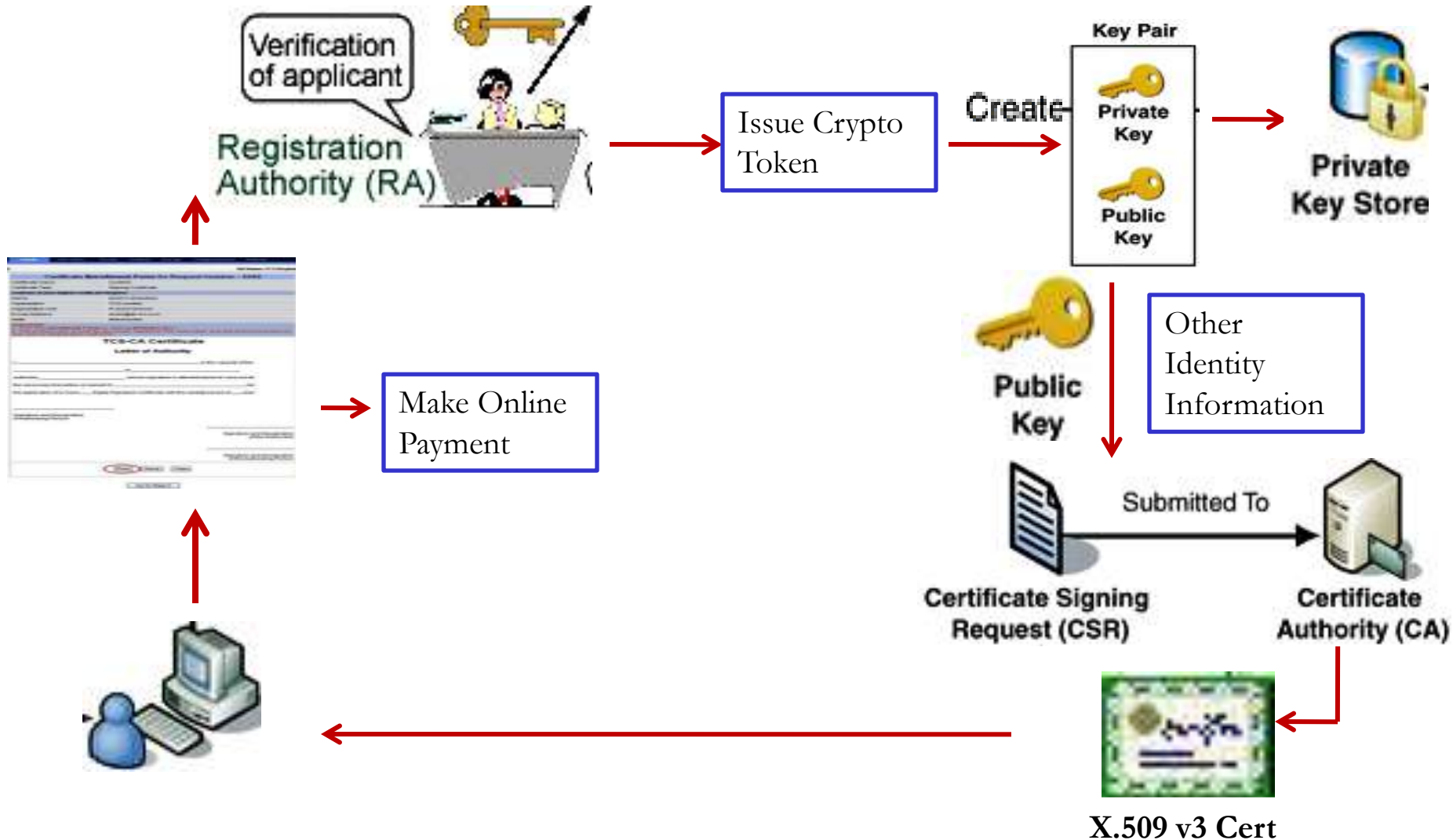
# Licensed CA's in India



- National Root CA (RCAI) – operated by **CCA**
  - Only issues CA certificates for licensed CAs
- CAs licensed under the National Root CA
  - National Informatics Centre (<https://nicca.nic.in>)
  - eMudhra ([www.e-mudhra.com](http://www.e-mudhra.com))
  - TCS ([www.tcs-ca.tcs.co.in](http://www.tcs-ca.tcs.co.in))
  - nCode Solutions CA([www.ncodesolutions.com](http://www.ncodesolutions.com))
  - SafeScript ([www.safescript.com](http://www.safescript.com))
  - IDRBT CA ([www.idbrtca.org.in](http://www.idbrtca.org.in))
  - C-DAC (<http://esign.cdac.in>) – Only e-Sign
- As of Jan, 2015 approx. 9 Million+ DSCs have been issued

# Certificate Issuance Process

# Certificate Issuance Process



# Types of Certificates





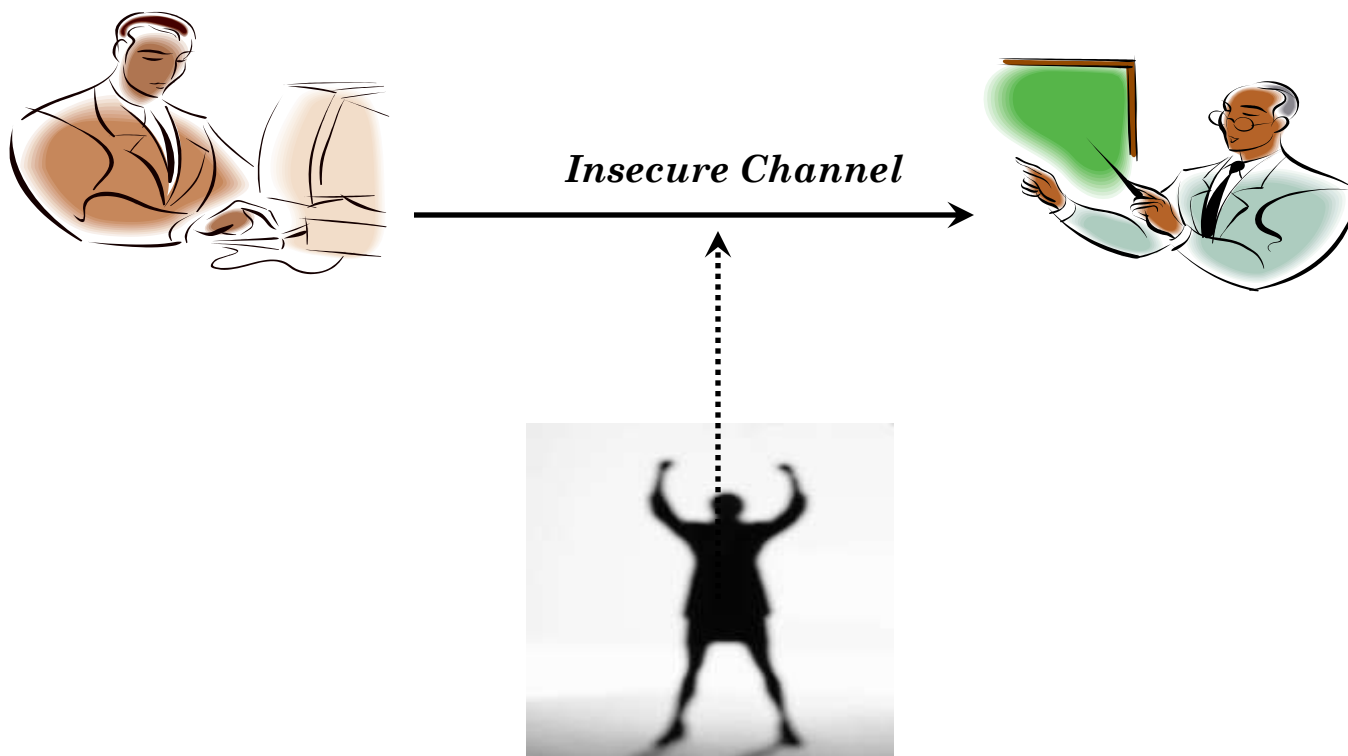
# Types of Certificates



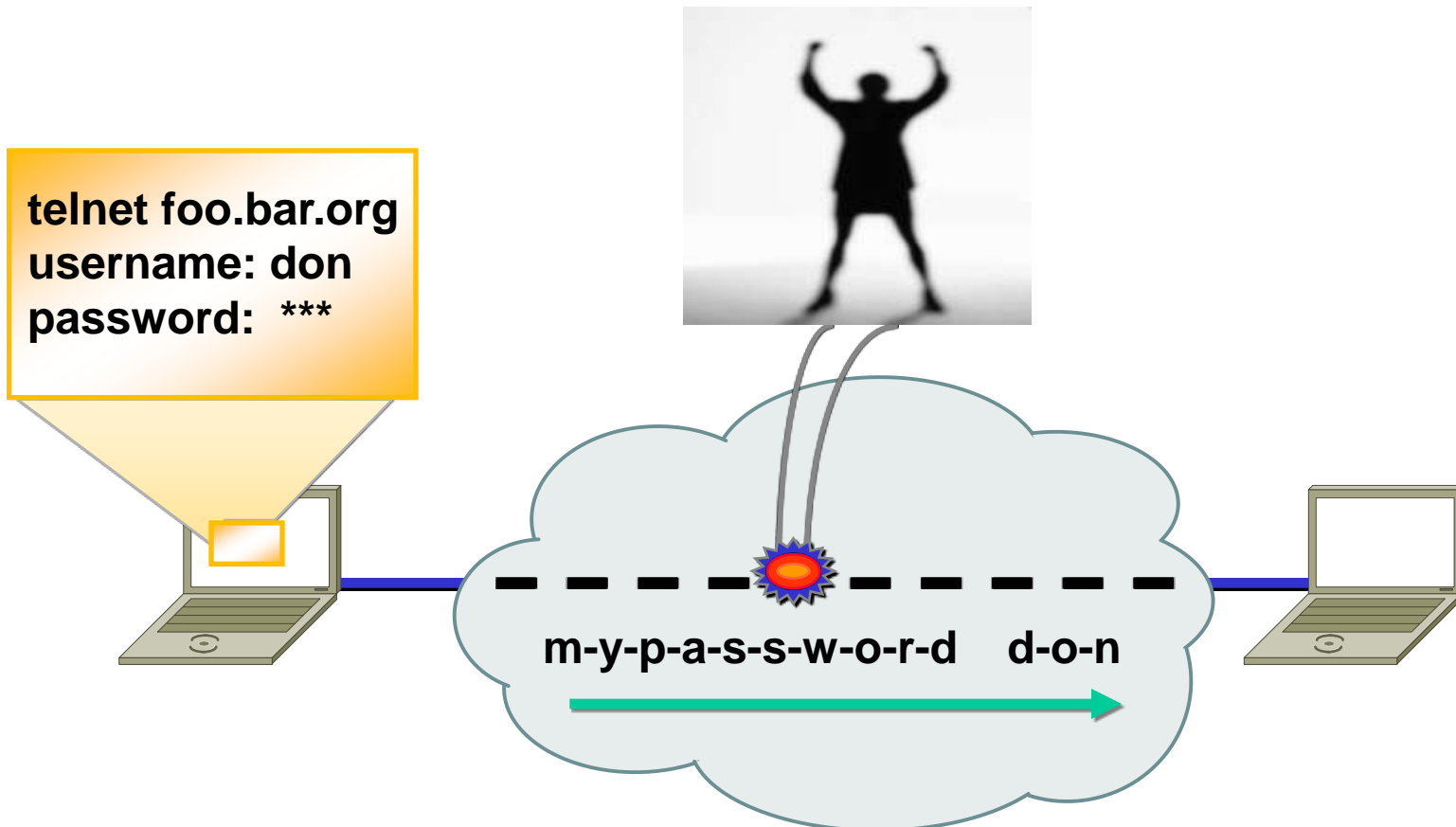
- Signing Certificate
  - Issued to a person for signing of electronic documents
- Encryption Certificate
  - Issued to a person for the purpose of Encryption;
- SSL Certificate
  - Issued to a Internet domain name (Web Servers, Email Servers etc...)

# Achieving Confidentiality

# Why you may need Secrecy ?

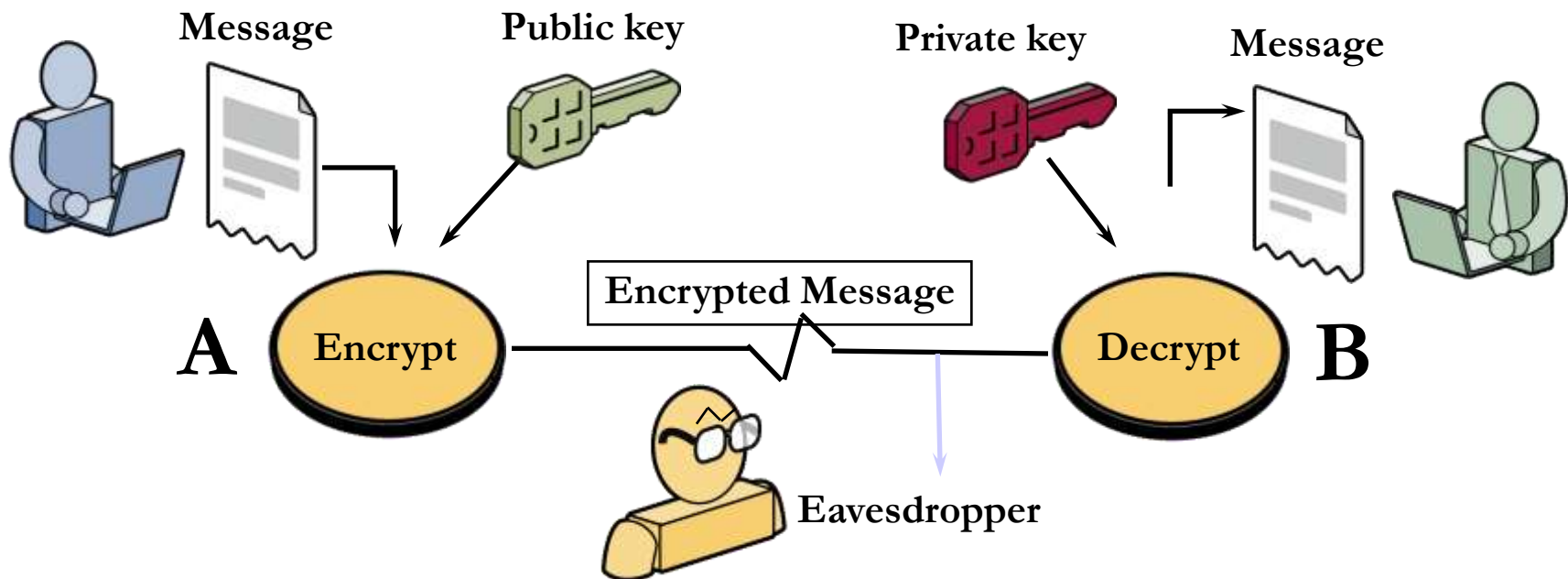


# Threats: Packet Sniffing



## Breach of Confidentiality

# Asymmetric Key Encryption - Confidentiality



# Encryption & Decryption (Asymmetric)



Jai

Veeru's Public  
Key

Message

Hi Veeru

I am Jai

Encryptor

**Gabbar**  
Encrypted Message  
#&23R\*7&#e

Veeru's  
Private Key



Veeru

Message

Hi Veeru

I am Jai

Decryptor





# General Conventions



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



# 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 **encryption certificate** to be used for encryption requirement as per his/her official capacity

# 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



# 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



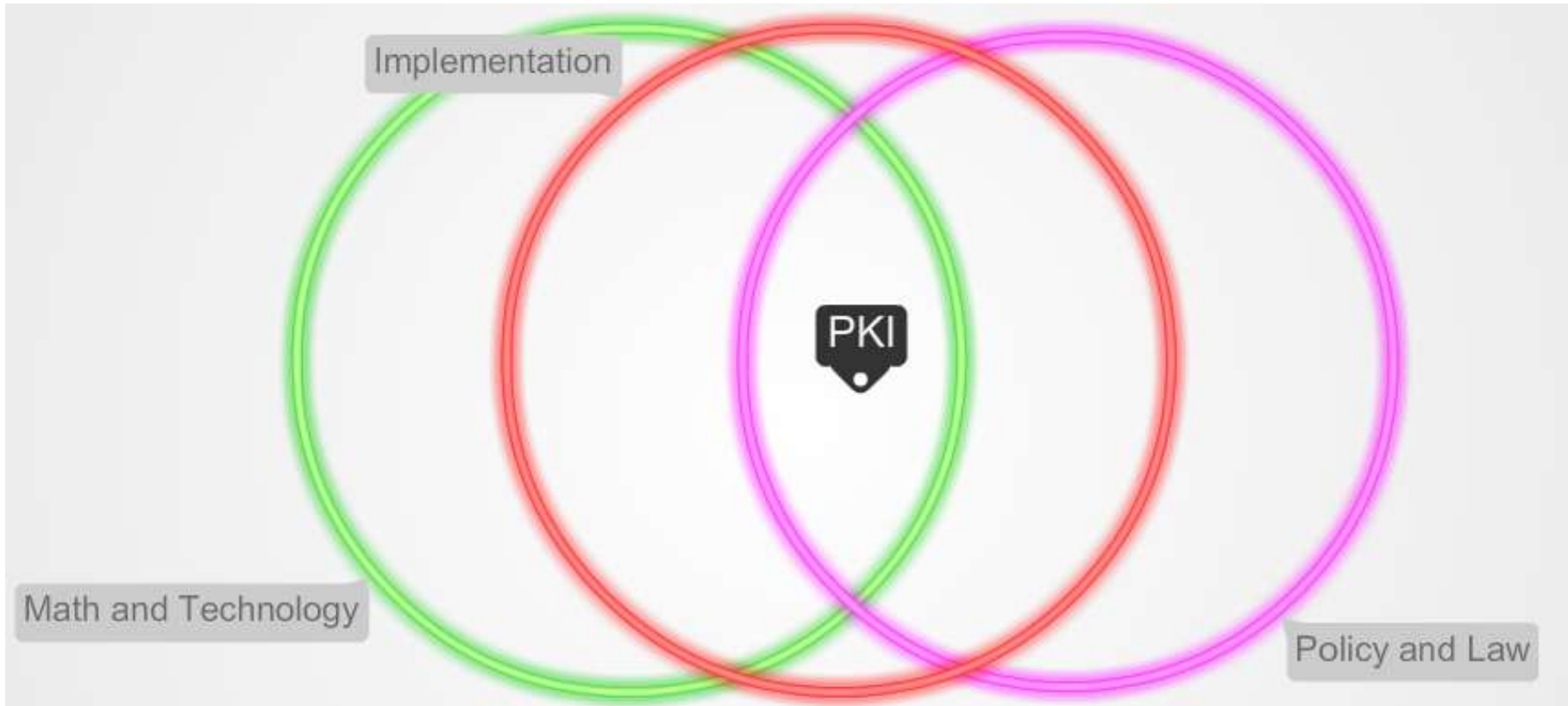
# Certificate Validation Methods



- Validating a certificate is typically carried out by PKI enabled application
- The validation process performs following checks
  - Digital signature of the issuer (CA)
  - Trust (Public Key verification) till root level
  - Time (Validity of the certificate)
  - Revocation (CRL verification)
  - Format



# Dimensions of PKI



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

# Present Digital Signature & PKI Implementations in India



# PKI enabled Applications



1	<b>e-Invoice</b>	(B2C)
2	<b>e-Tax Filing</b>	(G2C)
3	<b>e-Customs</b>	(G2B)
4	<b>e-Passport</b>	(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	<b>e-Governance</b>	<b>Bhoomi (G2C)</b> 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	<b>e-Payment</b>	(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	<b>e-Billing</b>	<b>(B2C)</b> -The electronic delivery and presentation of financial statement, bills, invoices, and related information sent by a company to its customers)
8	<b>e-Procurement</b>	<b>G2B , B2B</b>
9	<b>e-Insurance Service</b>	<b>(B2C)</b> - Presently the users are getting the E-Premium Receipts etc. which is digitally signed by the provider
10	<b>Treasury Operations</b>	<b>(G2C)</b> <i>Khajanae – II</i> of Govt. of Karnataka uses Digital Signatures to automate and speed up the treasury operations



## Other Implementations



- DGFT - Clearance of goods are now initiated by exporters through push of a button and in their offices;
  - Previously it used to take days; and requests are now cleared within 6 hours
- Indian Patent office has implemented e-filing of patents and allows only use of Class-3 Certificates
  - Around 30% of e-filing of patents is happening now, among the total filings.



# 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](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](http://www.cca.gov.in)
- e-Sign: <http://www.cca.gov.in/cca/?q=eSign.html>
- More Web Resources
  - Social Media: [www.facebook.com/pkiindia](https://www.facebook.com/pkiindia) [@pkiindia](https://twitter.com/pkiindia)

Thank You

pki@cdac.in