Digital Signatures and Public Key Infrastructure

Dr. Balaji Rajendran
Centre for Development of Advanced Computing (C-DAC)
Bangalore

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Agenda

- ✓ What & Why: Digital Signature?
- ✓ What is Digital Signature Certificate?
- ✓ Achieving Confidentiality
- ✓ Certifying Authority & Trust Model
- ✓ Certificate Issuance, Types, Classes
- ✓ Certificate Life Cycle Management and Validation Methods
- ✓ Risks and Precautions with DS
- ✓ Policy and Legal Aspects of PKI
- ✓ e-Sign – An Instant & Online way of Digital Signing in India
- ✓ PKI Applications in India

Understanding Signature

- Hand-written Signature – Definition & Purpose
  - A person's name written in a distinctive way as a form of **identification** in **authorizing** a cheque or document
  - A distinctive pattern, product, or characteristic by which someone or something can be **identified**

Characteristics of Hand 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

Attacks on Hand-written Signatures

- **Attacks on Integrity**
  - Content Alteration / Corruption !
- **Attacks on Identity**
  - Impersonation
  - How is Identity verified?
    - Authentication – Process of verifying who somebody is against his claim
      - **Identity is established / proved through Authentication!**

Attacks on Integrity

Note to kljfklsdajlkj direcljlkfjsdaar afafdasuoiae

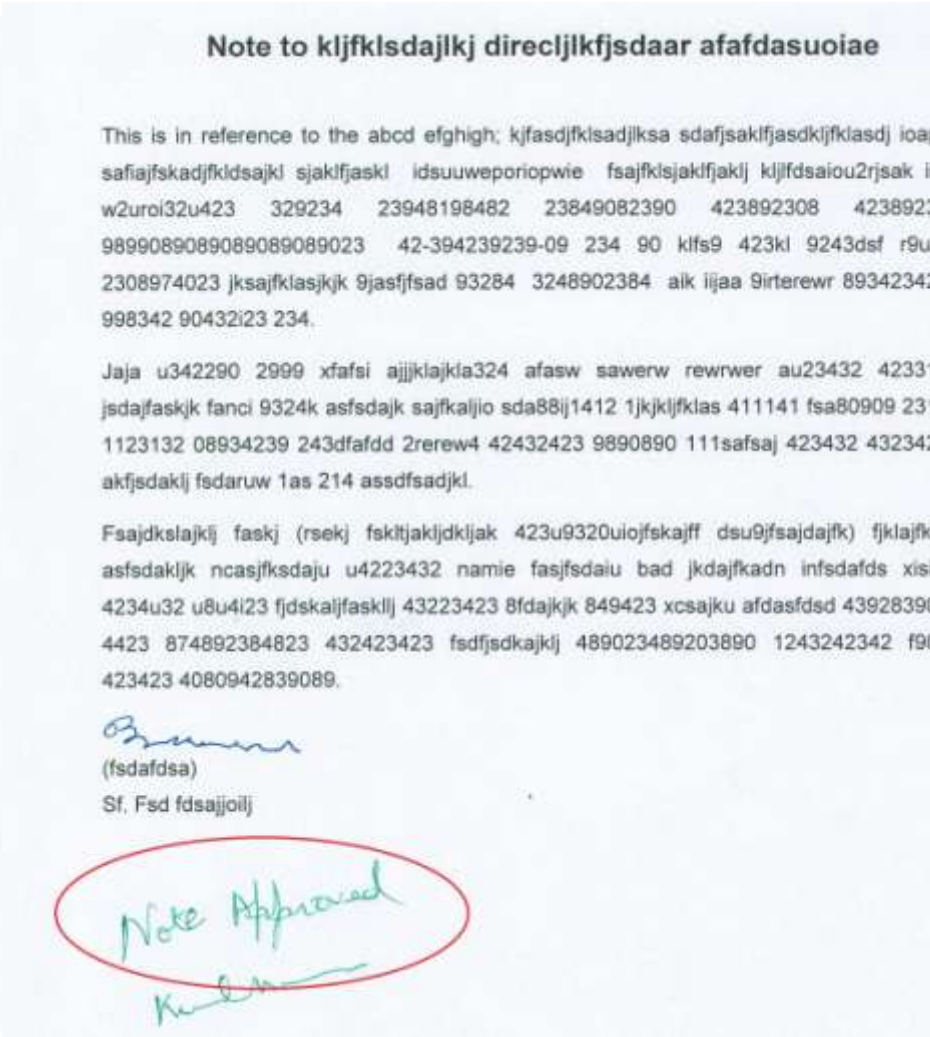
This is in reference to the abcd efghigh; kjfasdjfklsadjlksa sdafjsaklfjasdkljfklasdj ioapkafja safiajfskadjfkldsajkl sjaklfjaskl idsuuweporiopwie fsajfklsjaklfjaklj kljlfdsaiou2rjsak iiweop w2uroi32u423 329234 23948198482 23849082390 423892308 42389238094 9899089089089089089023 42-394239239-09 234 90 klfs9 423kl 9243dsf r9u23ur9 2308974023 jksajfklasjkjk 9jasfjfsad 93284 3248902384 aik iijaa 9irterewr 893423423432 998342 90432i23 234.

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

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

(fsdafdsa)
Sf. Fsd fdsajjoilj

Not Approved



Note to kljfklsdajlkj direcljlkfjsdaar afafdasuoiae

This is in reference to the abcd efghigh; kjfasdjfklsadjlksa sdafjsaklfjasdkljfklasdj ioa safiajfskadjfkldsajkl sjaklfjaskl idsuuweporiopwie fsajfklsjaklfjaklj kljlfdsaiou2rjsak i w2uroi32u423 329234 23948198482 23849082390 423892308 423892 9899089089089089089023 42-394239239-09 234 90 klfs9 423kl 9243dsf r9u 2308974023 jksajfklasjkjk 9jasfjfsad 93284 3248902384 aik iijaa 9irterewr 8934234 998342 90432i23 234.

Jaja u342290 2999 xfafsi ajjjklajkla324 afasw sawerw rewrwer au23432 4233 jsdajfaskjk fanci 9324k asfsdajk sajfkaljio sda88ij1412 1jkjkljfklas 411141 fsa80909 23 1123132 08934239 243dfafdd 2rerew4 42432423 9890890 111safsaj 423432 43234 akfjsdaklj fsdaruw 1as 214 assdfsadjkl.

Fsajdkslajklj faskj (rsekj fskltjakljdkljak 423u9320uiojfskajff dsu9jfsajdajfk) fjklajfk asfsdakljk ncasjfksdaju u4223432 namie fasjfsdaiu bad jkdajfkadn infsdafds xis 4234u32 u8u4i23 fjdskaljfaskllj 43223423 8fdajkjk 849423 xcsajku afdasfdsd 4392839 4423 874892384823 432423423 fsdfjsdkajklj 489023489203890 1243242342 f9 423423 4080942839089.

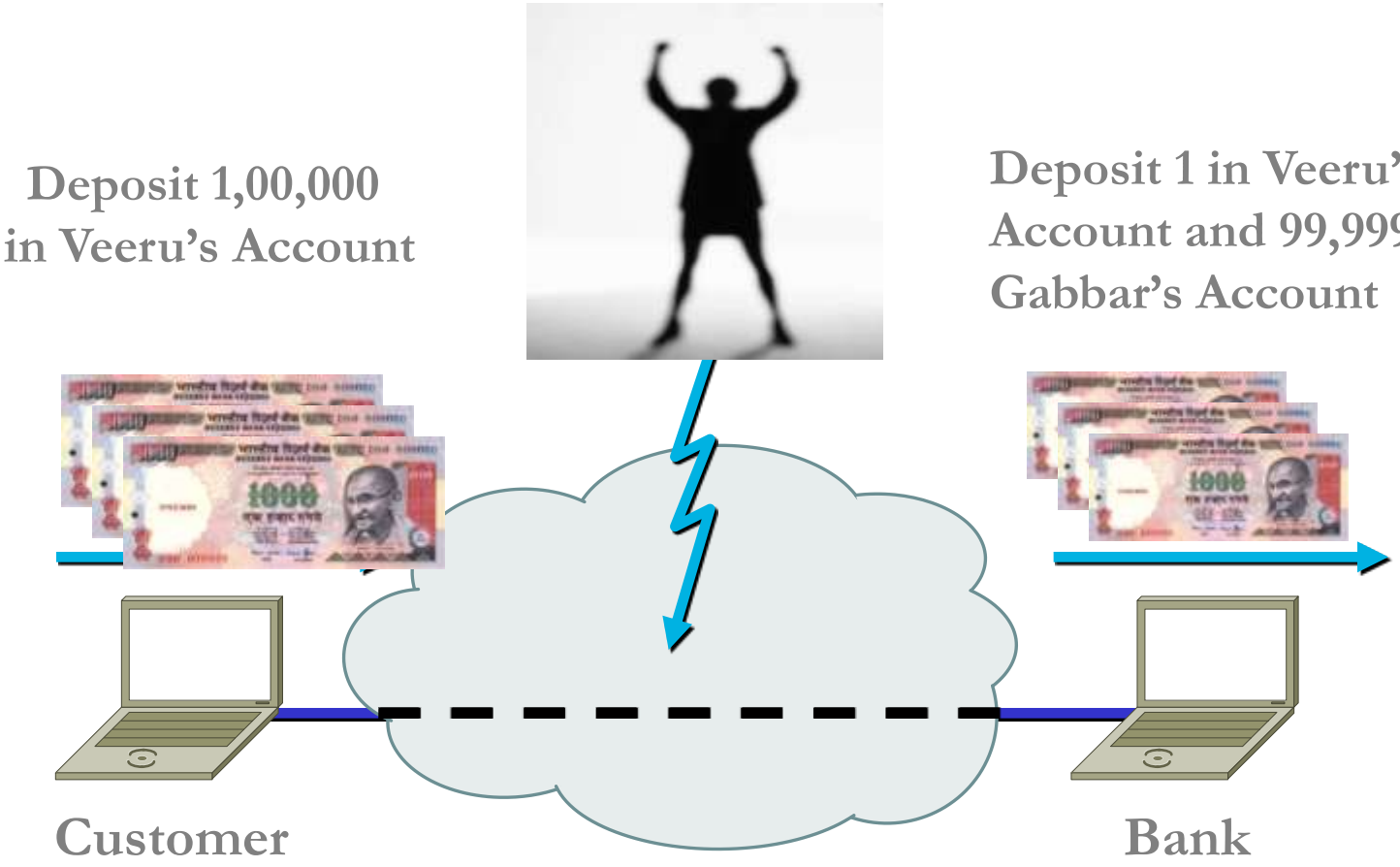
(fsdafdsa)
Sf. Fsd fdsajjoilj

Note Approved

Attacks on Integrity - 2

Electronic World

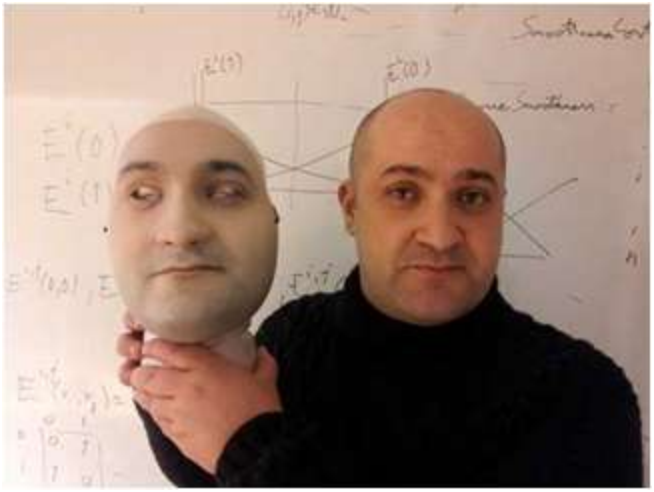
Attacks on Integrity



Breach of Integrity

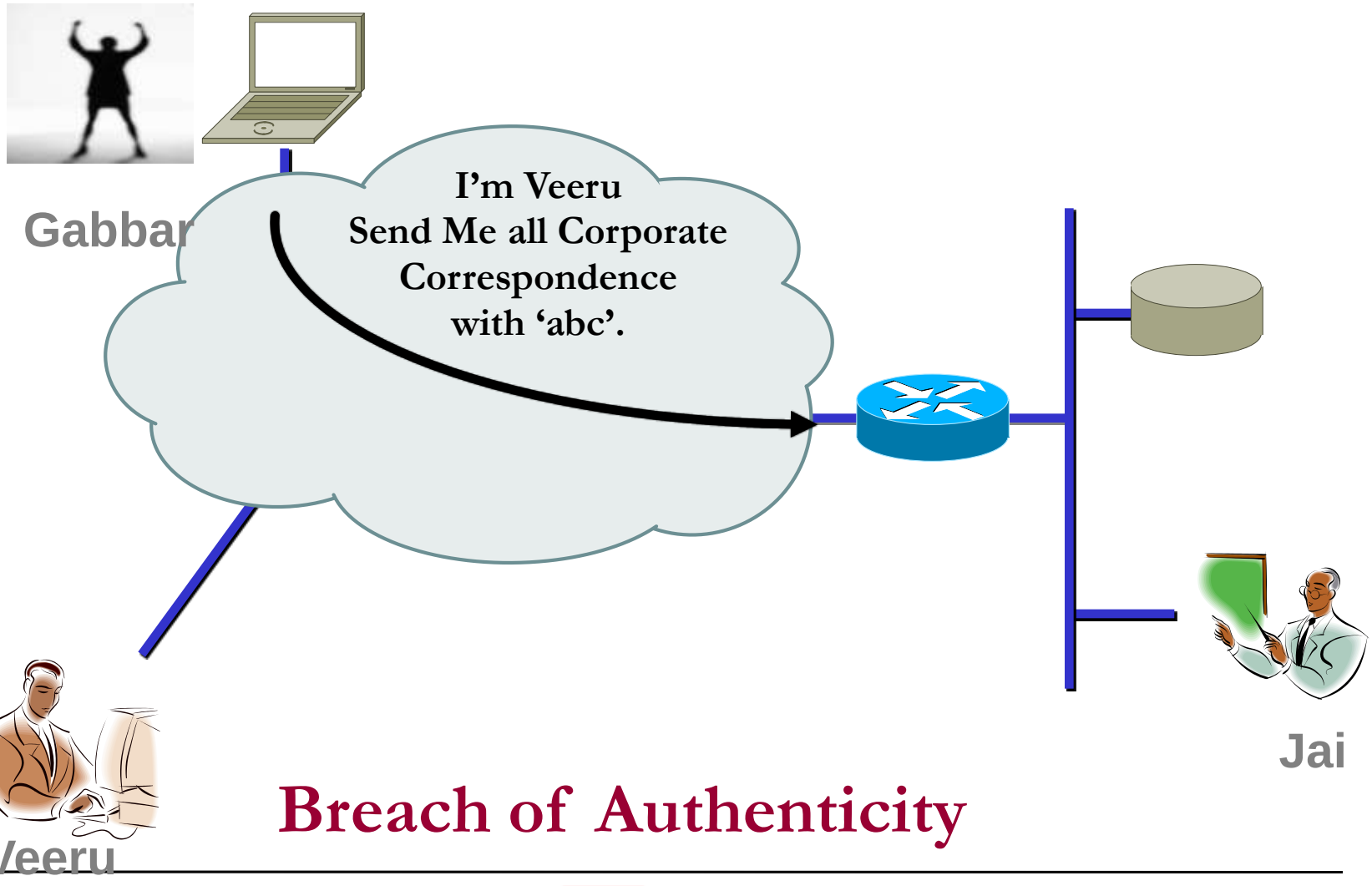
Attacks on Identity

- Spoofing!



Courtesy: Center for Machine Vision Research, Finland - http://www.oulu.fi/

Attacks on Identity



Breach of Authenticity

Basic Elements of Trust

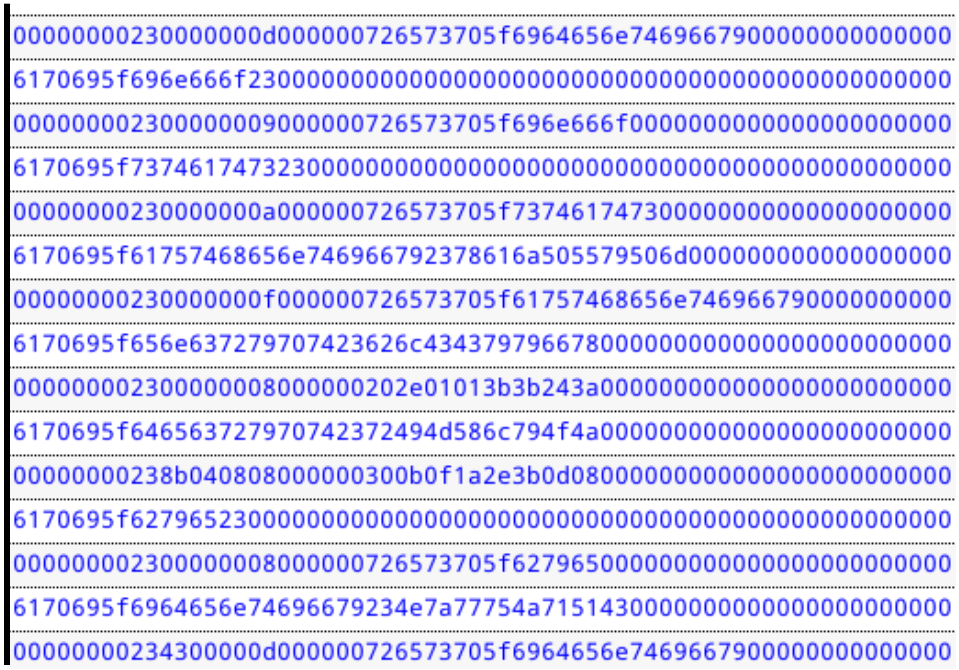
- **Privacy (Confidentiality):** Ensuring that **only authorized** persons read the Data/Message/Document
- **Authenticity:** Ensuring that Data/Message/Document originated from the **claimed** signer / sender
- **Integrity** : Ensuring that Data/Message/Document are **unaltered** by any unauthorized person
- **Non-Repudiation:** Ensuring that one **cannot deny** their signature or origination of a message

Digital Signatures

What is a 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
  - Verifiable
  - Provides Authentication
  - Provides Data Integrity
  - Provides Non-repudiation



Creating Digital Signature

- Every individual is given a pair of **keys**
  - ***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***

Asymmetric Key Cryptography

- Keys in a Key pair are mathematically related to each other
  - If one of the key in a key pair is used for Encryption (or Decryption) then the other key should be used for decryption (or Encryption)
- Also known as **Public Key Cryptography**
- Knowledge of the ***encryption key*** doesn't give you knowledge of the ***decryption key***

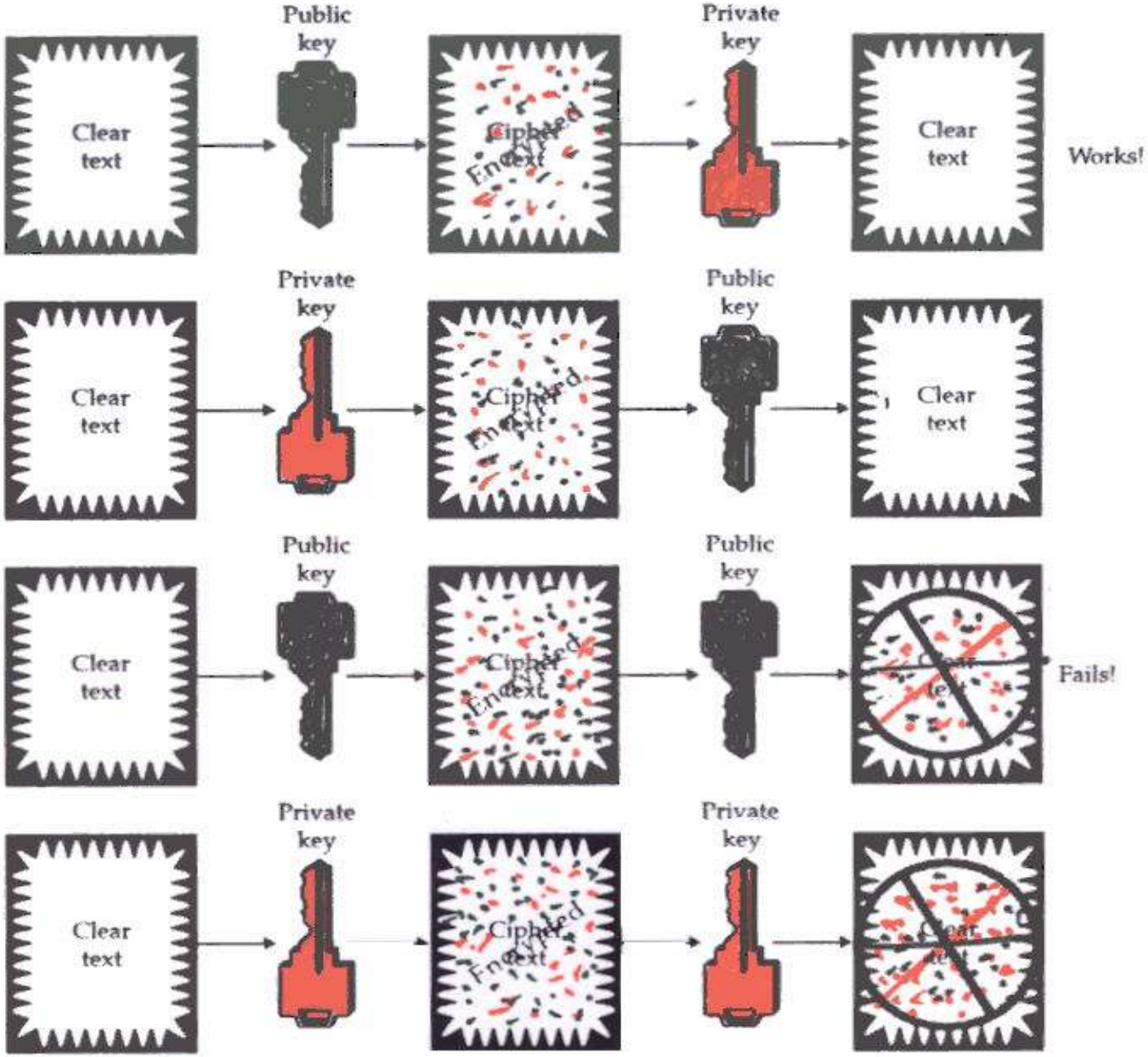
What is a key pair?

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
```

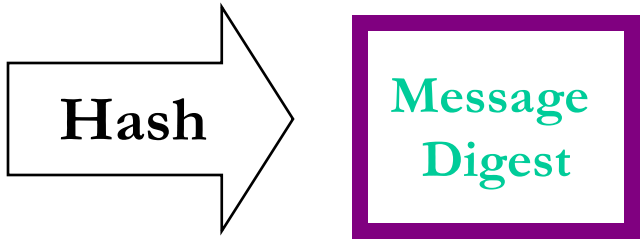
Public Key

```
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
```


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

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 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 pm. Veeru

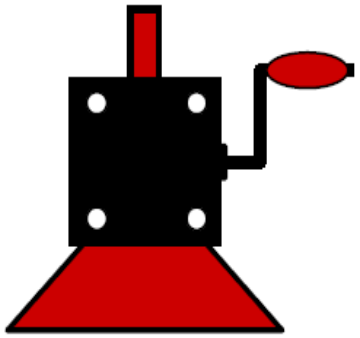
Message Digest

B5EA1EC376E61DB2680D0312FC26D3773F384E43	86D19C25294FB0D3E4CF8A026823439064598009

Digests are Different

Hash – One-way

B5EA1EC376E61DB2680D0312FC26D3773F384E43



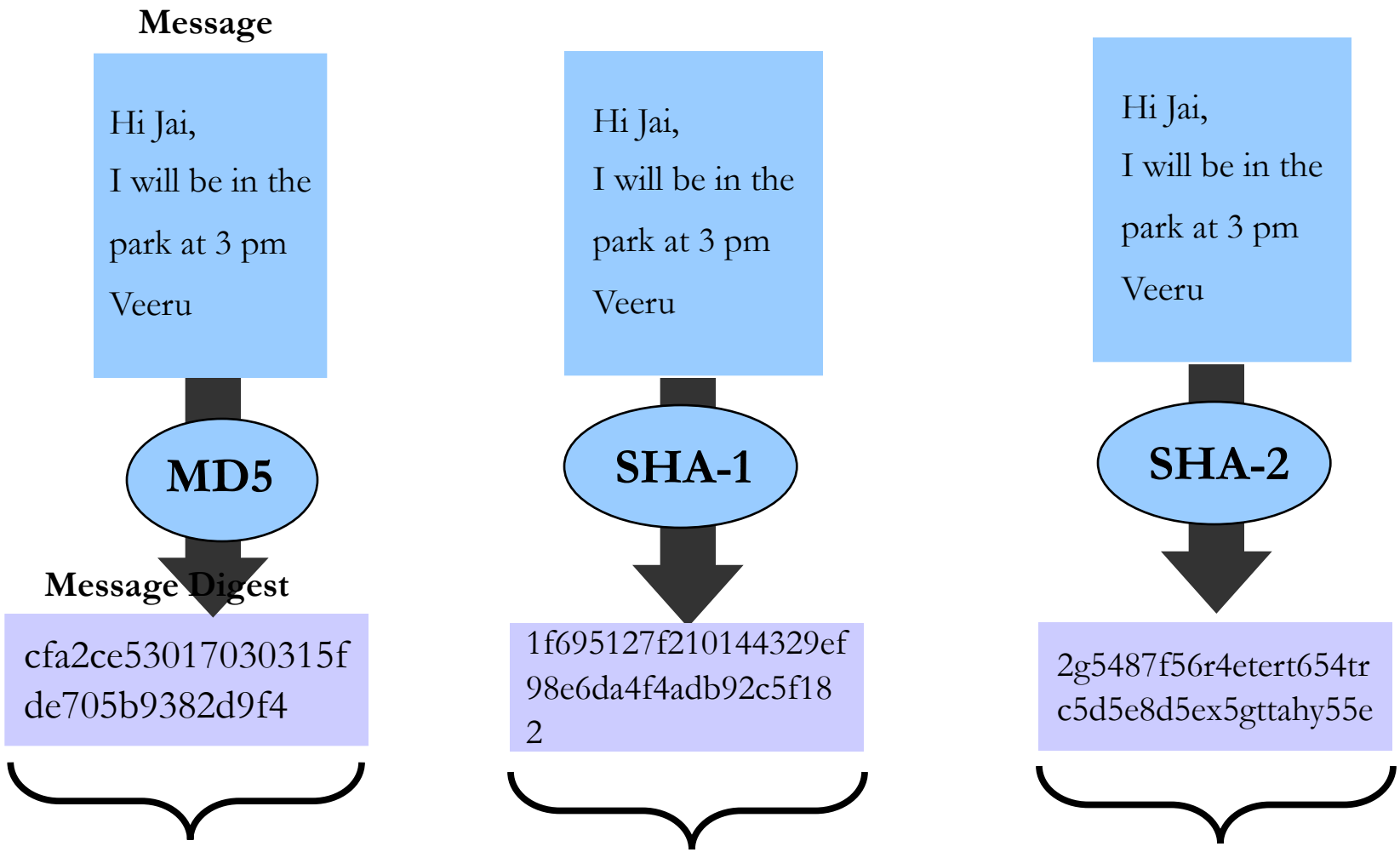
Hi Jai

I will be in the park at

3 pm

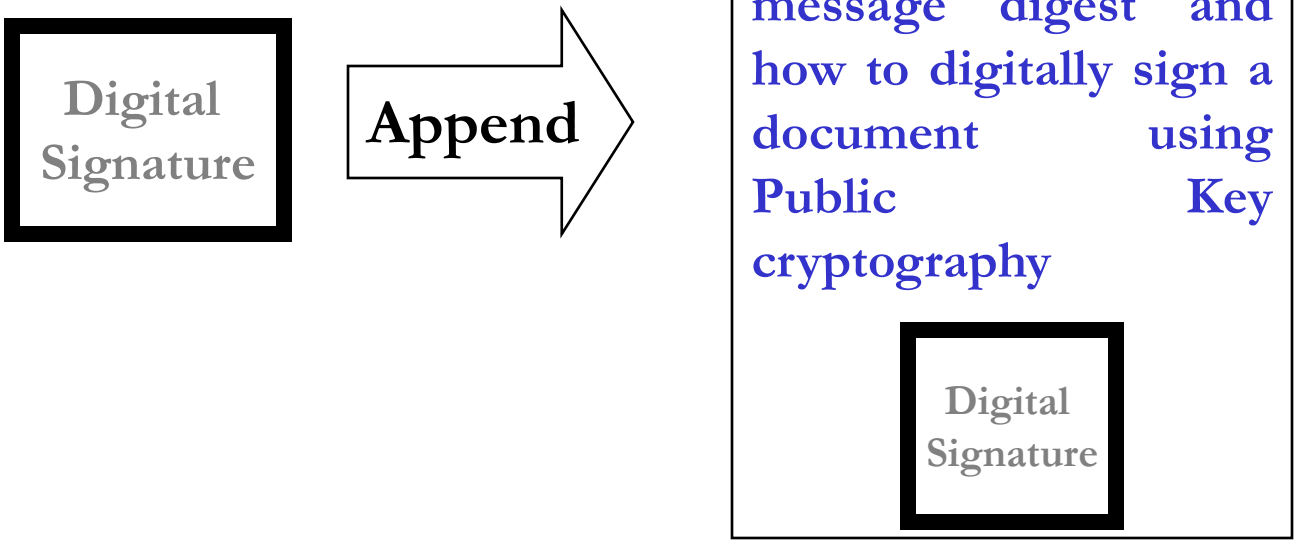
Veeru

MD5 and SHA

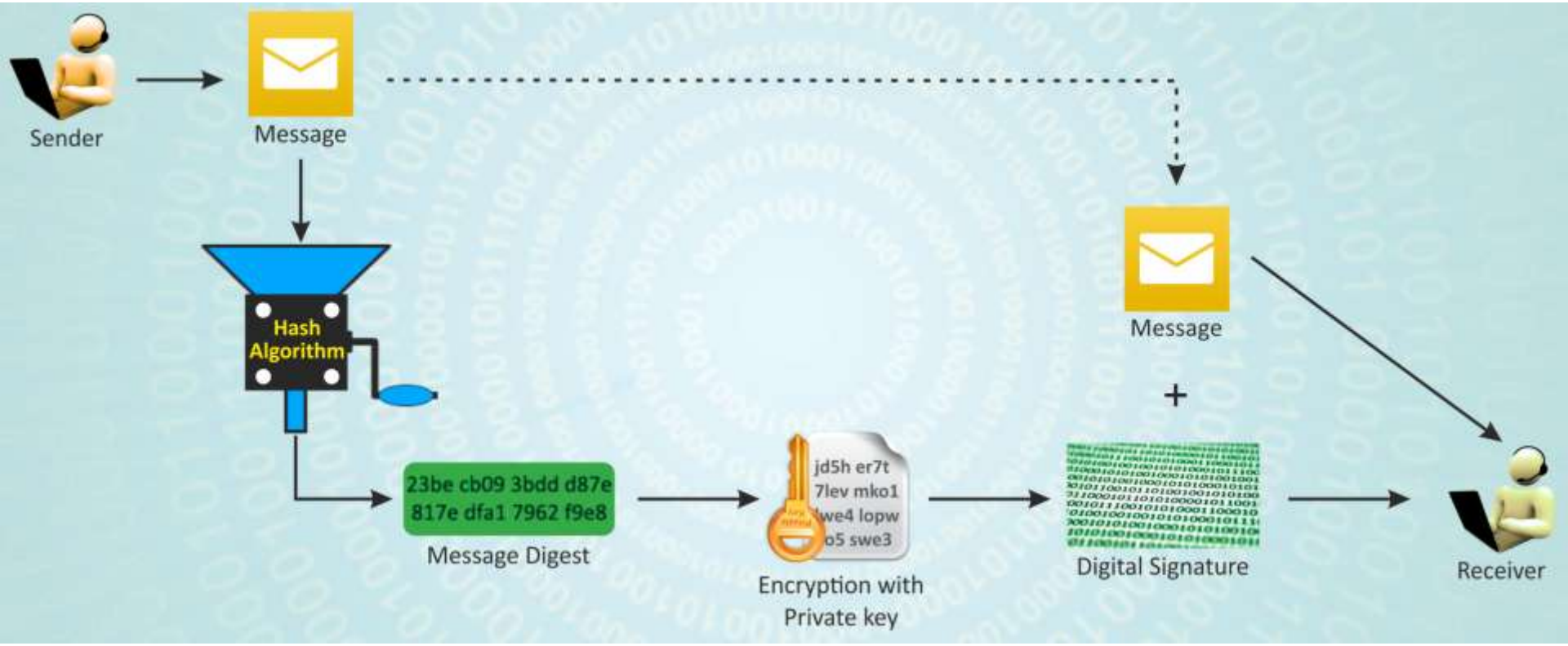

Message
Hi Jai,
I will be in the
park at 3 pm
Veeru
MD5
Message Digest
cfa2ce53017030315f
de705b9382d9f4
128 Bits
Hi Jai,
I will be in the
park at 3 pm
Veeru
SHA-1
1f695127f210144329ef
98e6da4f4adb92c5f18
2
160 Bits
Hi Jai,
I will be in the
park at 3 pm
Veeru
SHA-2
2g5487f56r4etert654tr
c5d5e8d5ex5gttahy55e
224/256/384/512

Digital Signing – Step 2

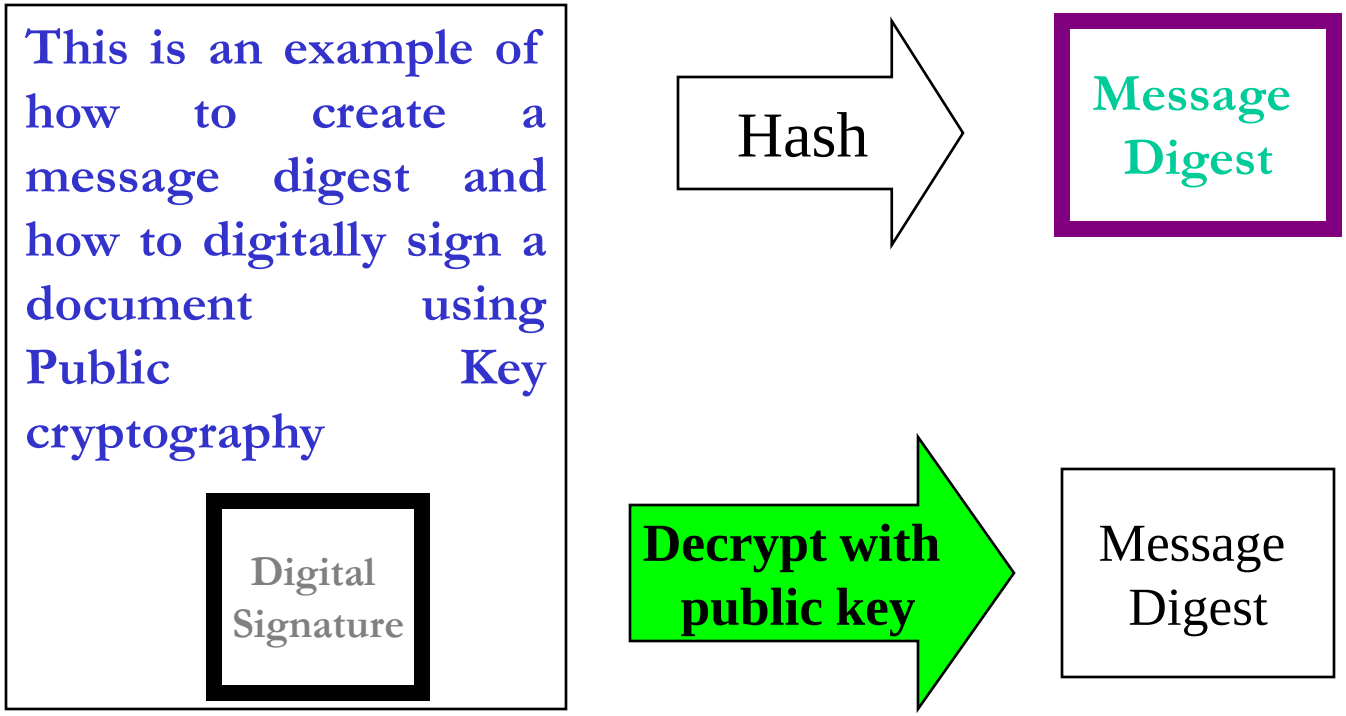
Digital Signing – Step 3



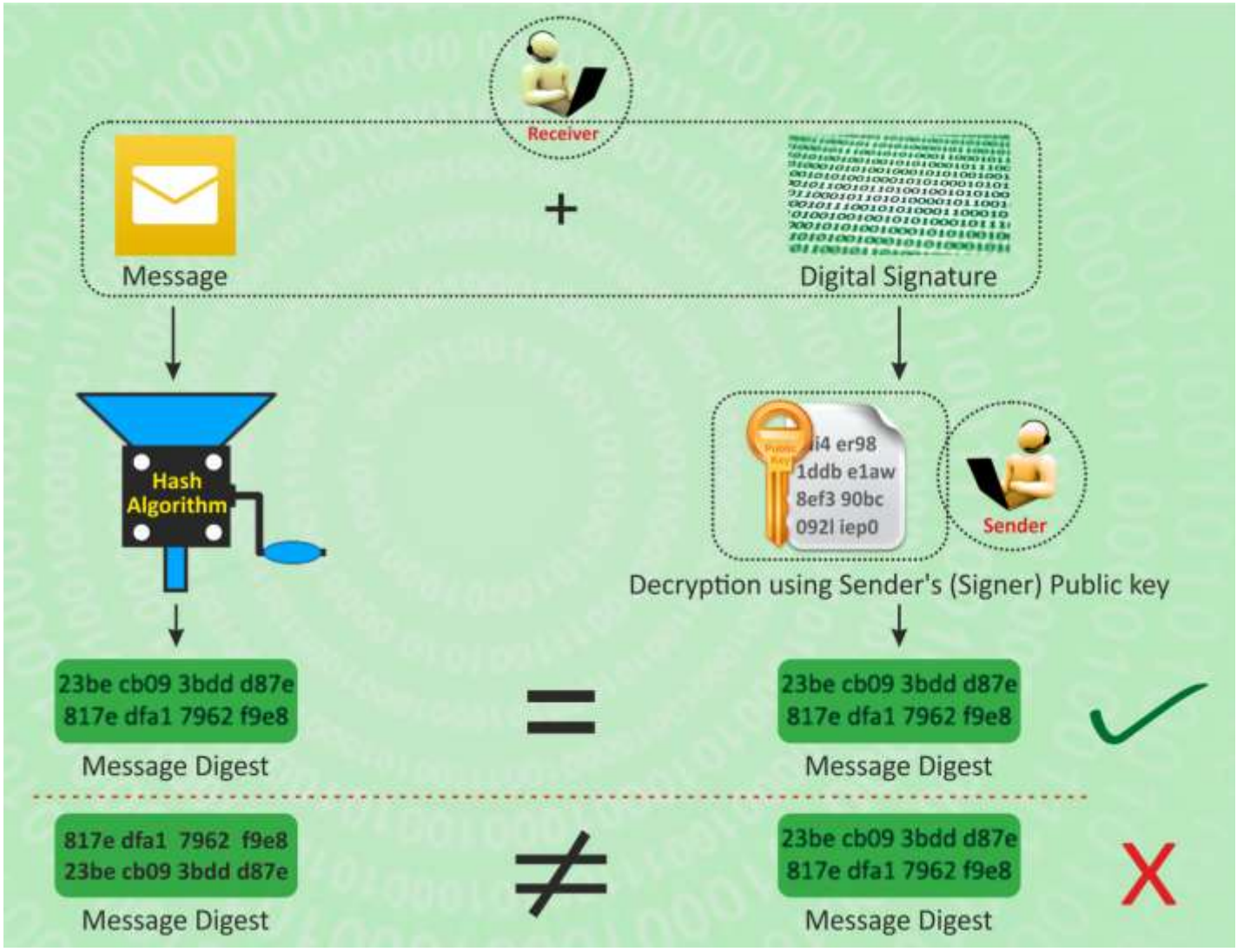
Digital Signing Process



Digital Signature Verification



Digital Signature Verification



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 Signatures - Recap

- Establishes
  - **Identity and Authenticity** of the Signer
  - **Integrity** of the document
  - **Non-Repudiation** (inability to deny being signed) to **a certain extent**
- General Conventions
  - **Signing – Private Key of the Signer**
  - **Verification – Public Key of the Signer**

Digital Signature Certificate (DSC)

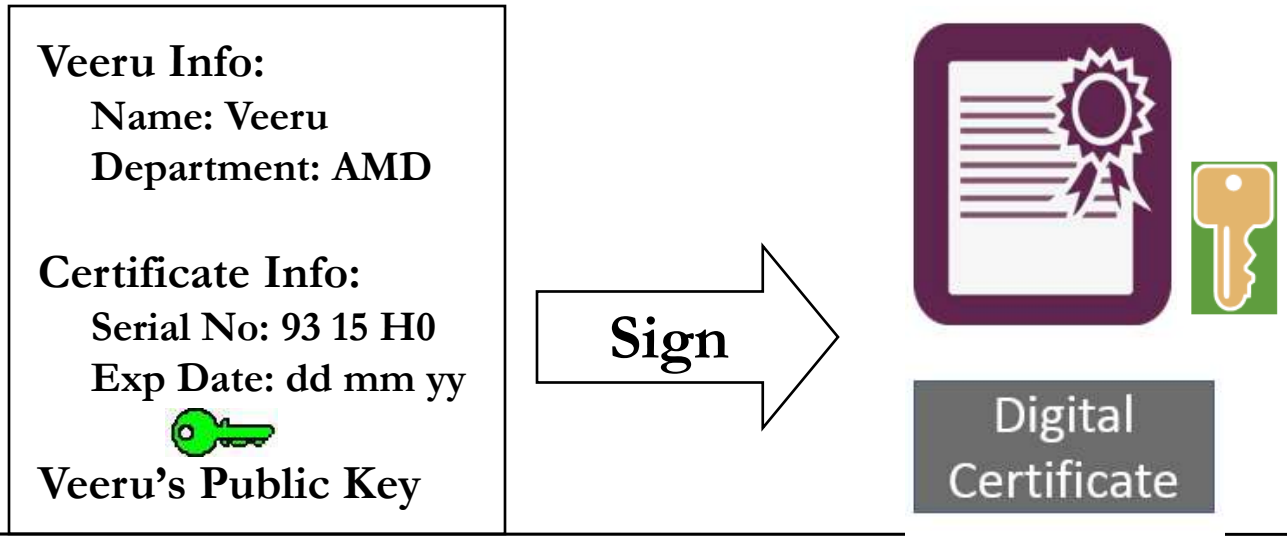
Why do we need DSC?

- To firmly establish the ownership of public key
- To certify and provide a strong mechanism for non-repudiation (to inability to deny)

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.



Certifying Authority (CA) ?

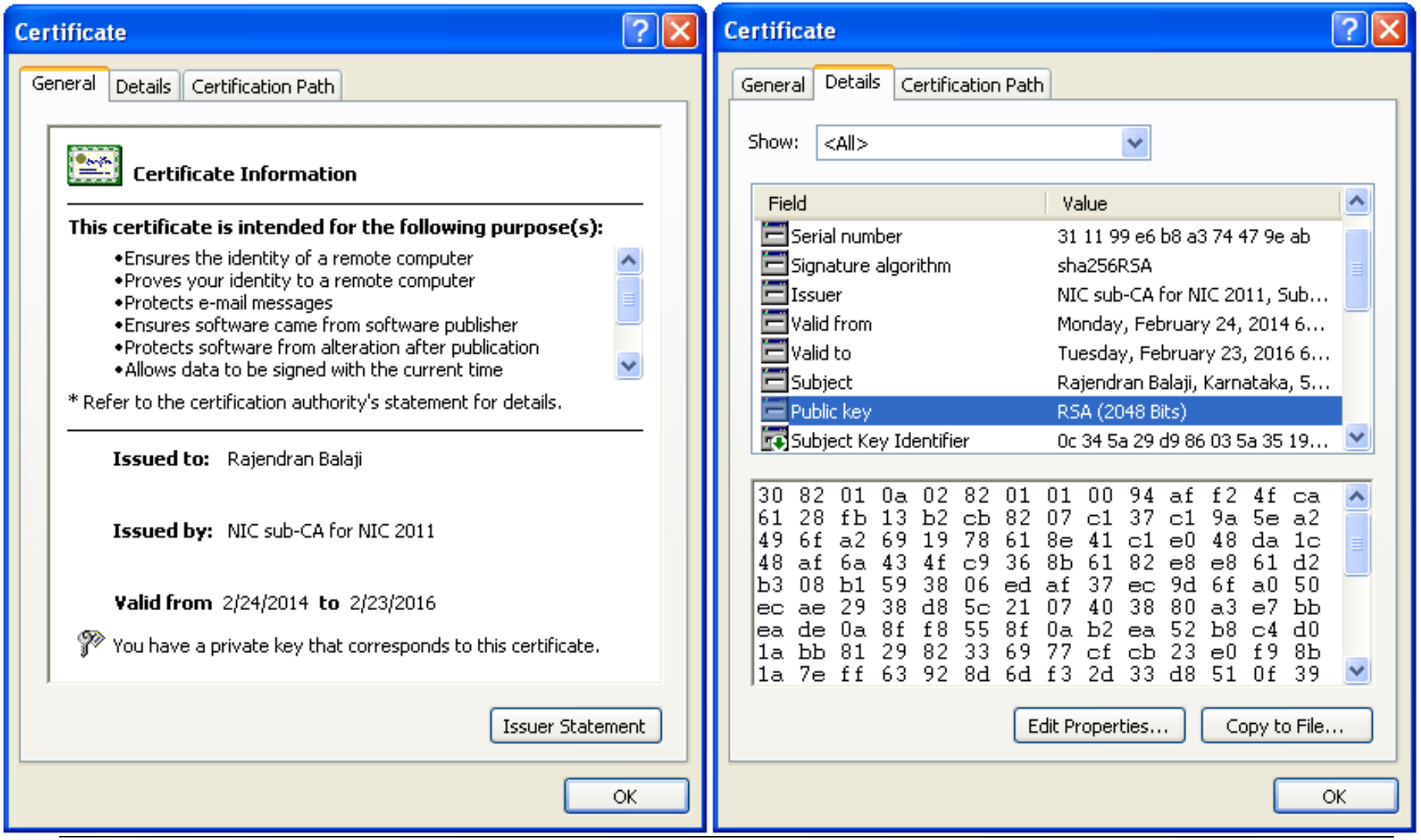
Certifying Authority (CA)

- Certifying authority is an entity which issues Digital Signature Certificate **(DSC)**
- It is a **trusted third party**
- CA's are the important components 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



Digital Signatures and PKI - II

Over to Mr. Subhrakanti Kaviraj

Conclusion

- PKI and Digital Signatures have been transforming the way traditional transactions happen
- PKI Ecosystem has the potential to usher
  - Transparency
  - Accountability
  - Time, Cost & Effort-savings
  - Speed of execution and to be an integral part of
  - **Digital India and bring in Digital Identity**

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
- e-Sign: http://www.cca.gov.in/cca/?q=eSign.html

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

Thank You

pki@cdac.in

www.facebook.com/pkiindia

PKIIndia

@pkiindia