Digital Signatures and PKI

Dr. Mohammed Misbahuddin

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

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Agenda

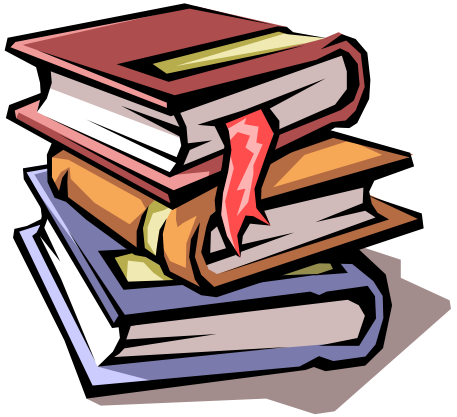
- ✓ What & Why: Digital Signature?
- ✓ What is Digital Signature Certificate?
- ✓ Certifying Authority & Trust Model
- ✓ Certificate Issuance, Types, Classes
- ✓ Certificate Life Cycle Management and Validation Methods
- ✓ Achieving Confidentiality
- ✓ Dimensions of PKI
- ✓ PKI Applications in India

Purpose of Signing

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

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

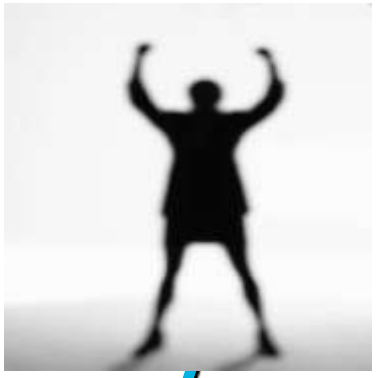
Authenticity: Ensuring that Data/Message/Document are genuine

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

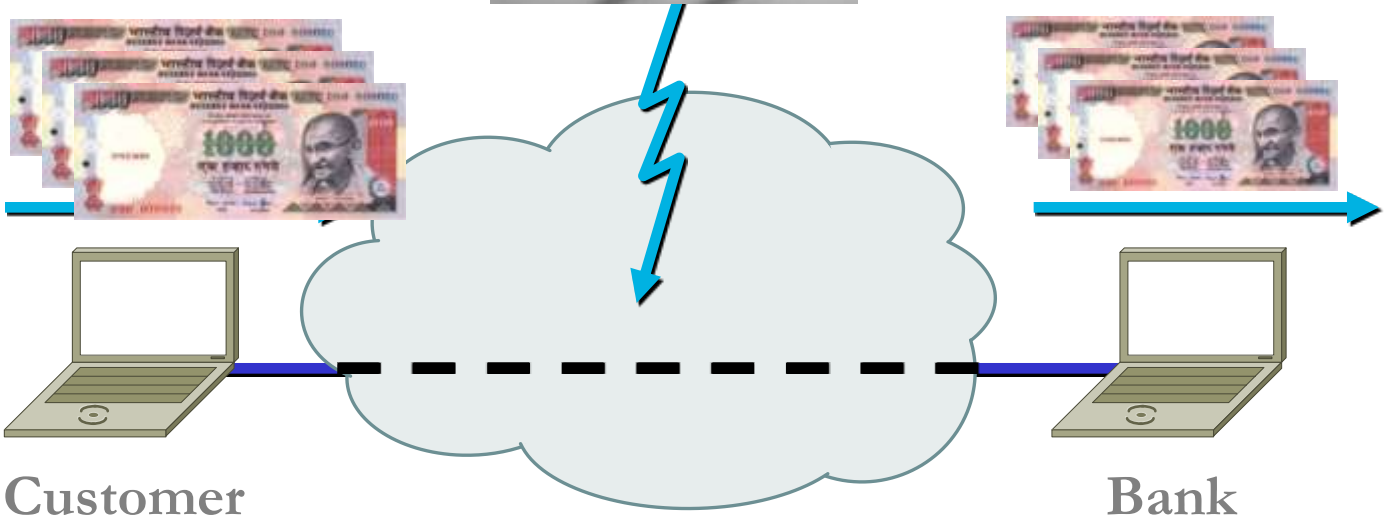
Non-Repudiation: Ensuring that one party of a transaction cannot deny having sent a message

Threats: Data Alteration

Deposit 1,00,000
in Veeru's Account



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

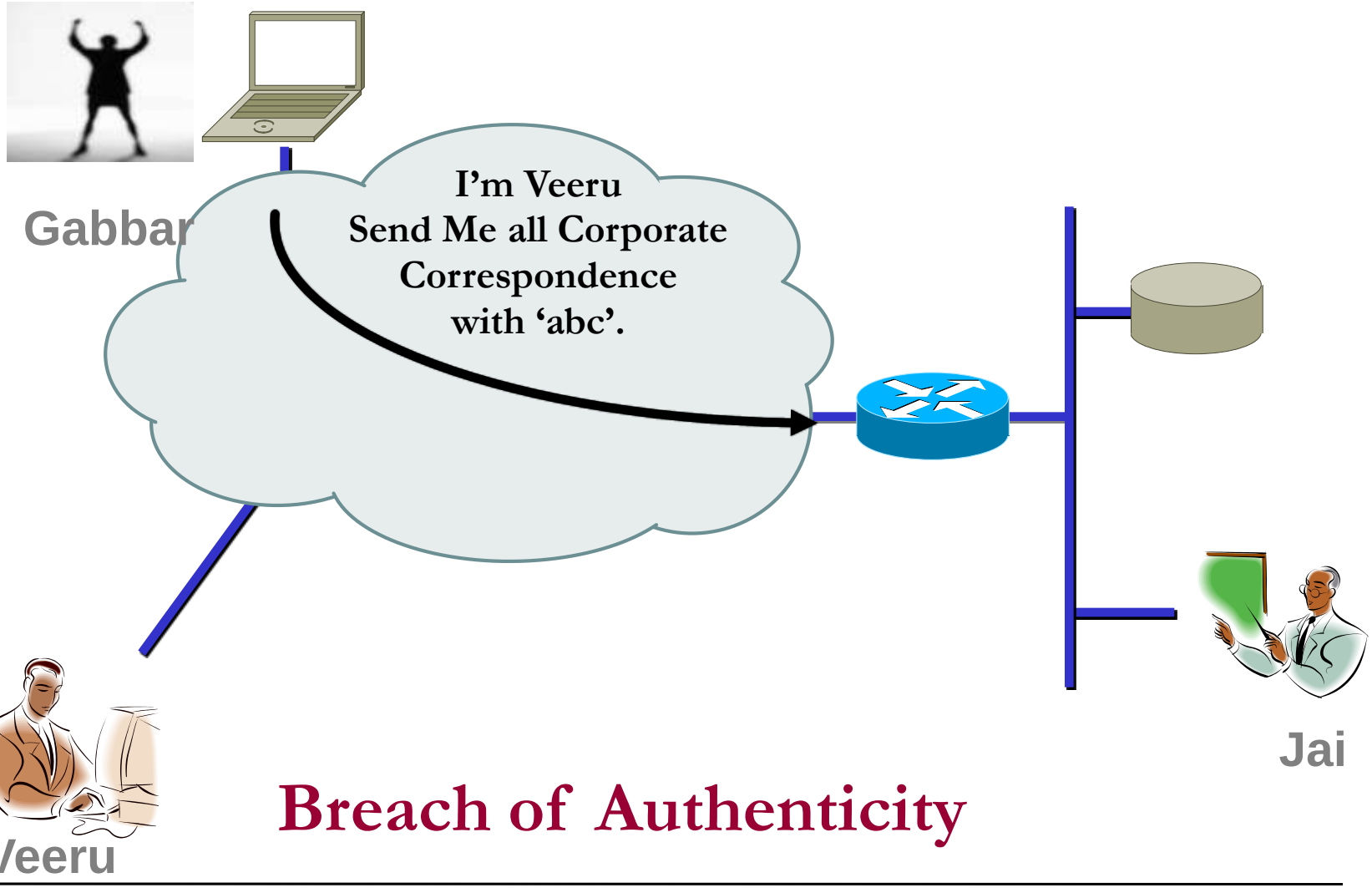


Customer

Bank

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

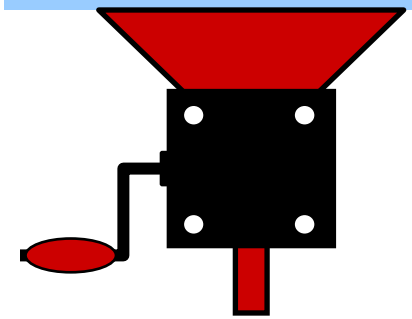
Message

Hi Jai,

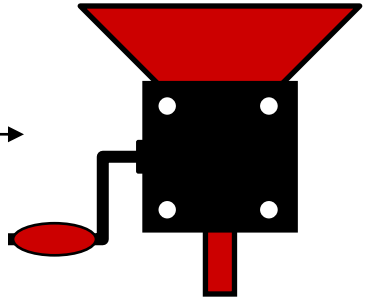
I will be in the park at

3 pm.

Veeru



← Hash Algorithm →



Message Digest

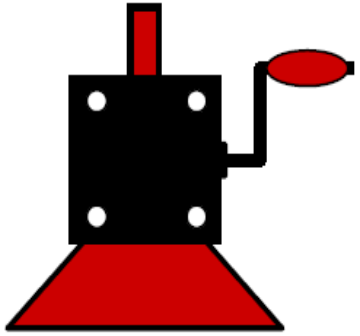
B5EA1EC376E61DB2680D0312FC26D3773F384E43

86D19C25294FB0D3E4CF8A026823439064598009

Digests are Different

Hash – One-way

B5EA1EC376E61DB2680D0312FC26D3773F384E43



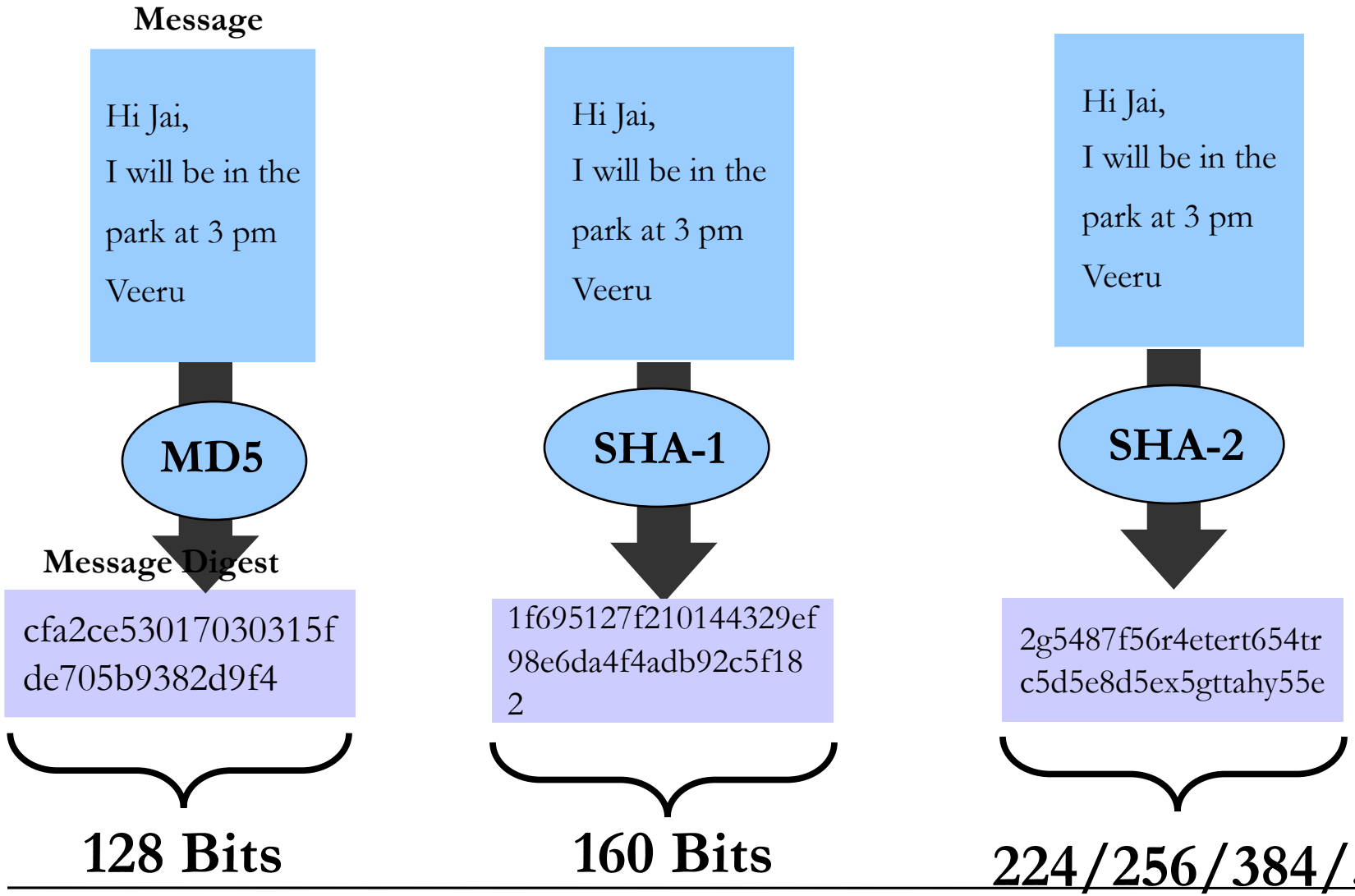
Hi Jai

I will be in the park at

3 pm

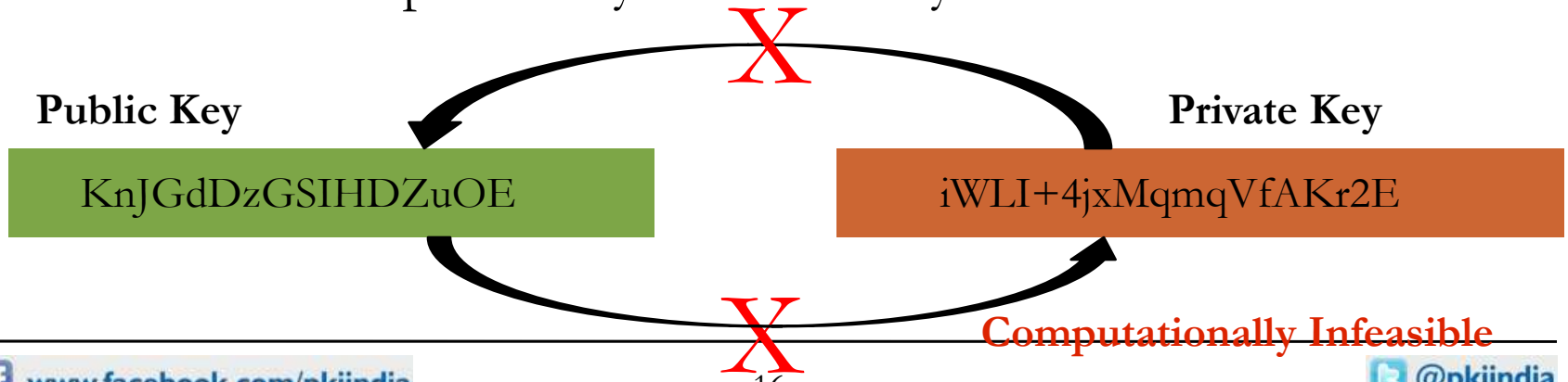
Veeru

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

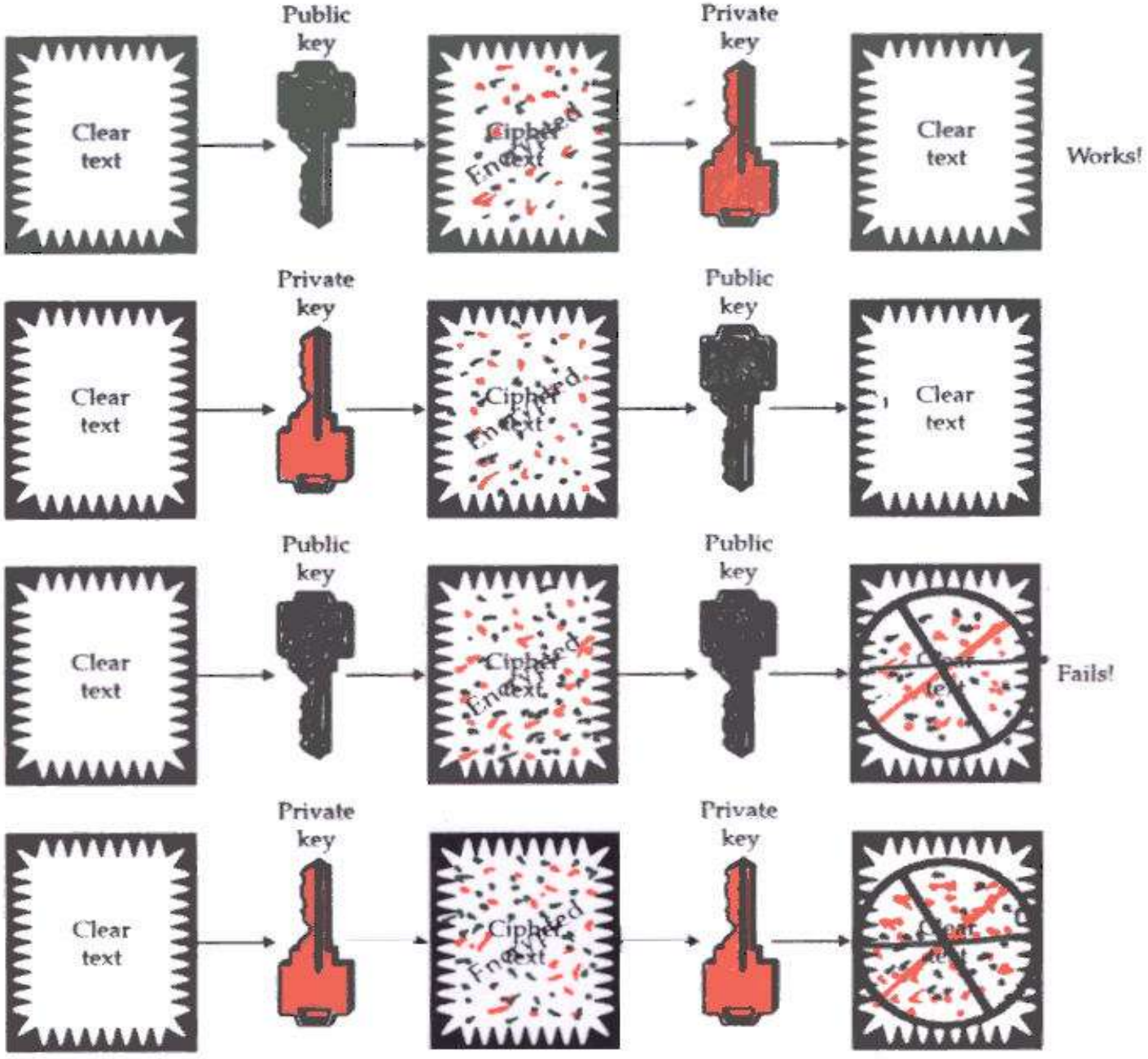
(including Algorithm identifier) [2048 bit]

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
```


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	*A* should know	*B* 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

Loss of 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 ioapkaf safiajfskadjfkldsajkl sjaklfjaskl idsuuweporiopwie fsajfklsjaklfjaklj kljlfdsaiou2rjsak iiwe w2uroi32u423 329234 23948198482 23849082390 423892308 423892380 9899089089089089089023 42-394239239-09 234 90 klfs9 423kl 9243dsf r9u23u 2308974023 jksajfklasjkjk 9jasfjfsad 93284 3248902384 aik iijaa 9irterewr 8934234234 998342 90432i23 234.

Jaja u342290 2999 xfafsi ajjjklajkla324 afasw sawerw rewrwer au23432 4233123 jsdajfaskjk fanci 9324k asfsdajk sajfkaljio sda88ij1412 1jkjkljfklas 411141 fsa80909 23112 1123132 08934239 243dfafdd 2rerew4 42432423 9890890 111safsaj 423432 43234234 akfjsdaklj fsdaruw 1as 214 assdfsadjkl.

Fsajdkslajklj faskj (rsekj fskltjakljdkljak 423u9320uiojfskajff dsu9jfsajdajfk) fjklajfkdlaj asfsdakljk ncasjfksdaju u4223432 namie fasjfsdaiu bad jkdajfkadn infsdafds xisityeu 4234u32 u8u4i23 fjdskaljfaskllj 43223423 8fdajkjk 849423 xcsajku afdasfdsd 4392839044 4423 874892384823 432423423 fsdfjsdkajklj 489023489203890 1243242342 f9089 423423 4080942839089.

(fsdafdsa)
Sf. Fsd fdsajjoilj

Note Approved

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

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

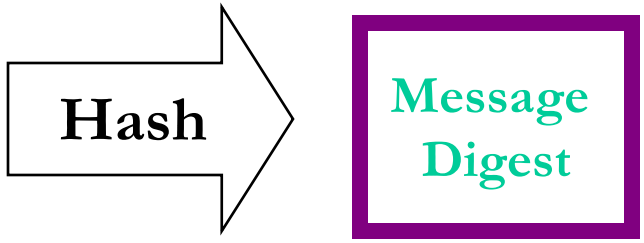
Creating Digital Signature

- 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

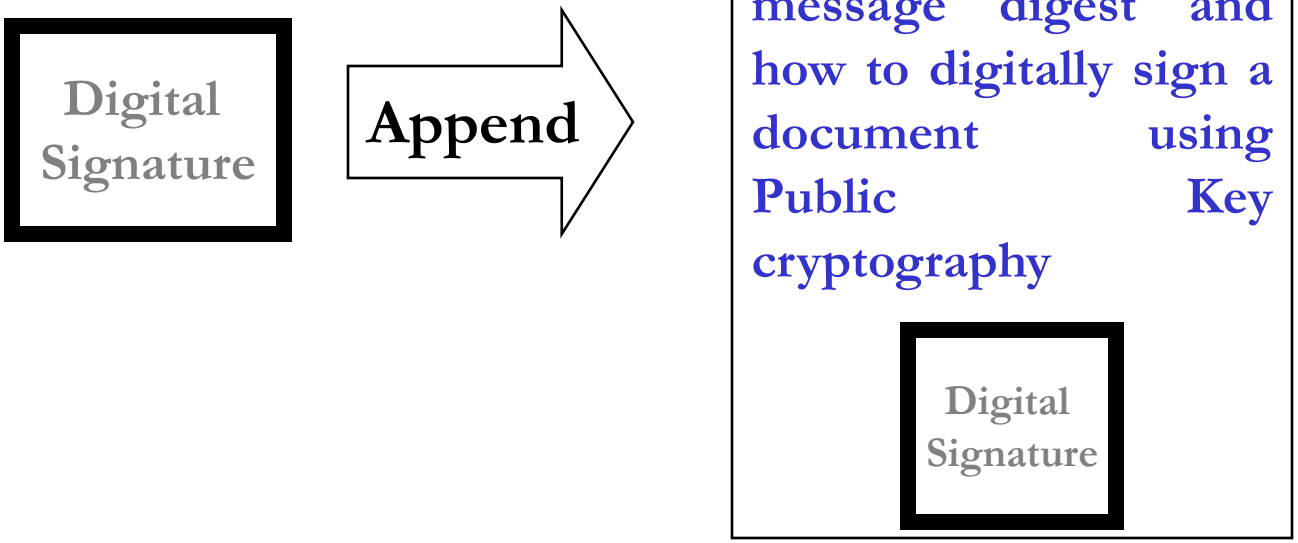
Digital Signing – Step 1

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

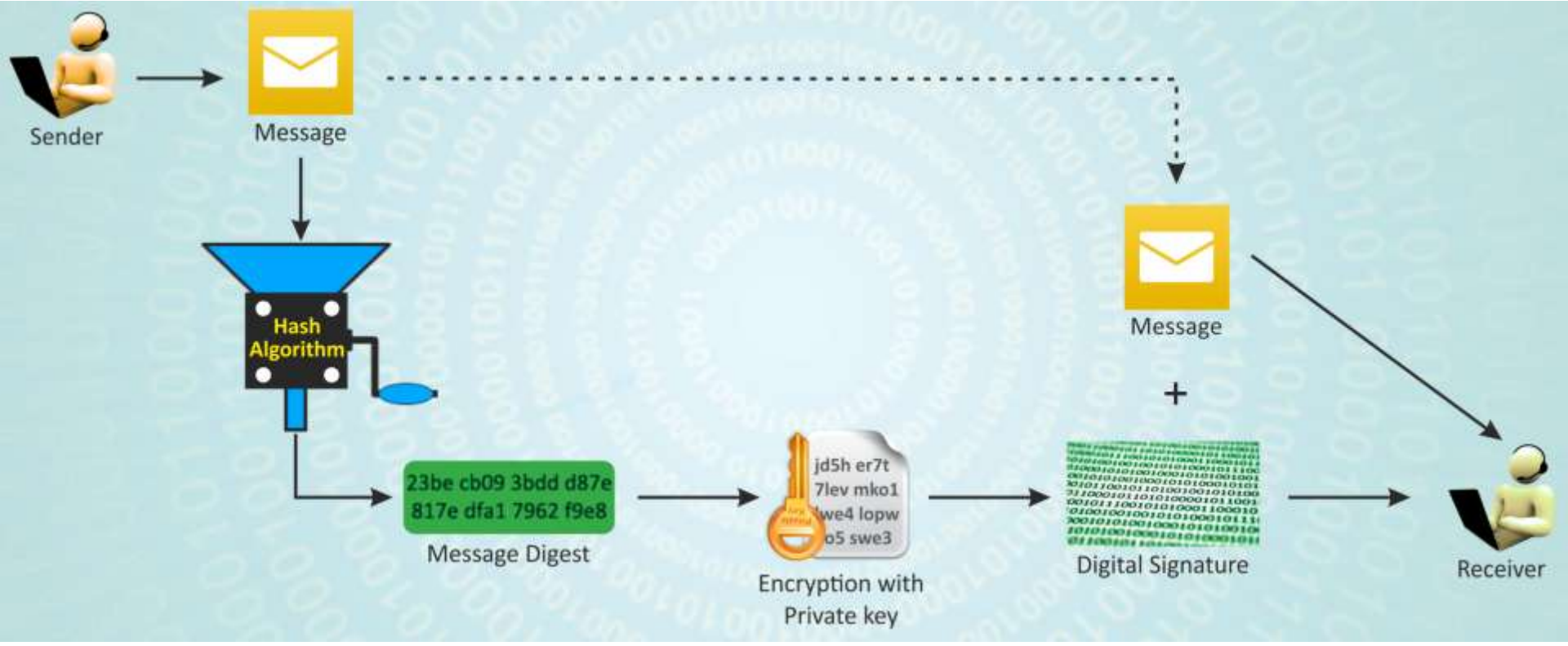


Digital Signing – Step 2

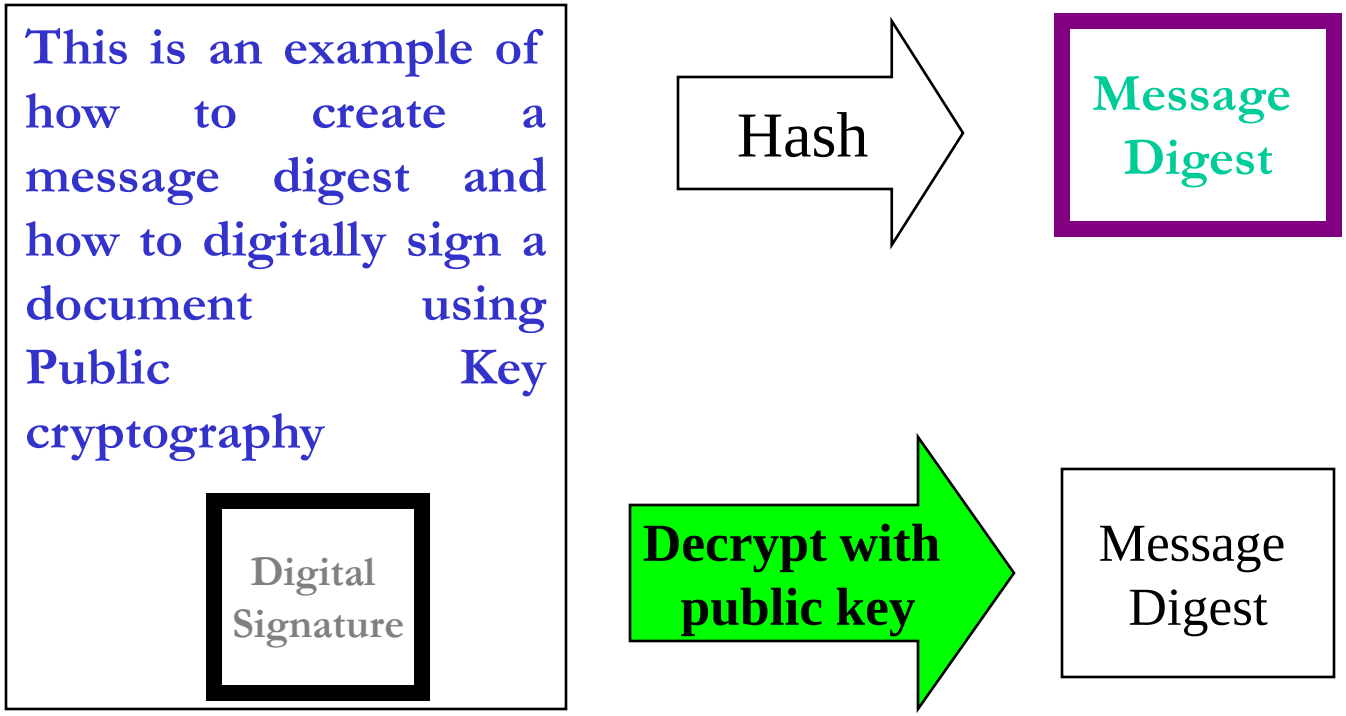
Digital Signing – Step 3



Digital Signing Process



Digital Signature Verification



Loss of 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.

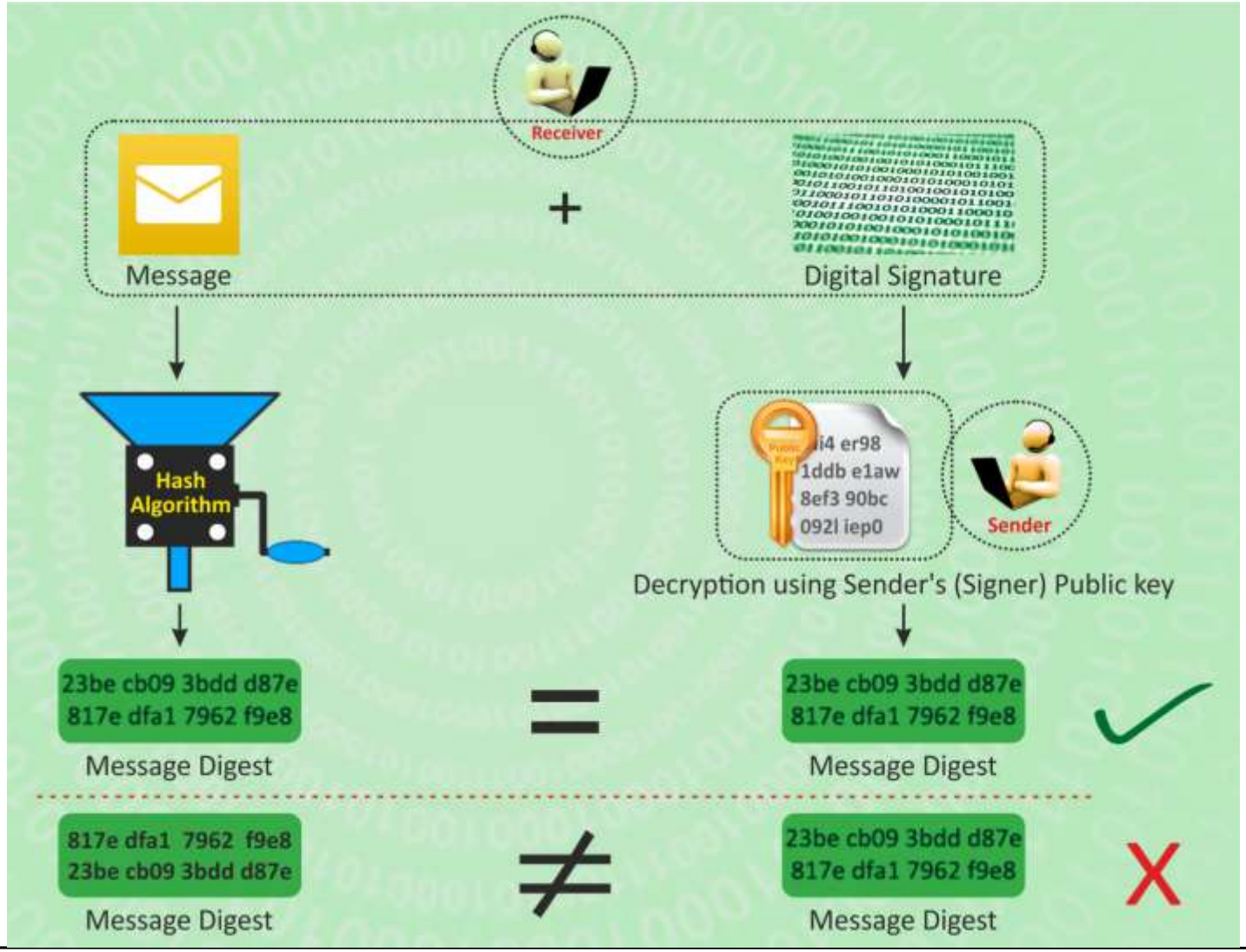
Jaja u342290 2999 xfafsi ajjjklajkla324 afasw sawerw rewrwer au23432 4233 jsdajfaskjk fanci 9324k asfsdajk sajfkaljio sda88ij1412 1jkjkljfklas 411141 fsa80909 23 1123132 08934239 243dfafdd 2rerew4 42432423 9890890 111safsaj 423432 43234 akfjsdaklj fsdaruw 1as 214 assdfsadjkl.

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

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**

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.

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
- More Web Resources
  - Social Media: www.facebook.com/pkiindia @pkiindia

Thank You

pki@cdac.in