ECOMMERCE-DIGITAL SIGANTURES

Class: II BCA

Mrs. C.Pradeepa
Assistant Professor
Department of Computer Applications

SRI AKILANDESWARI WOMEN'S COLLEGE, WANDIWASH
SWAMY ABEDHANADHA EDUCATIONAL TRUST, WANDIWASH

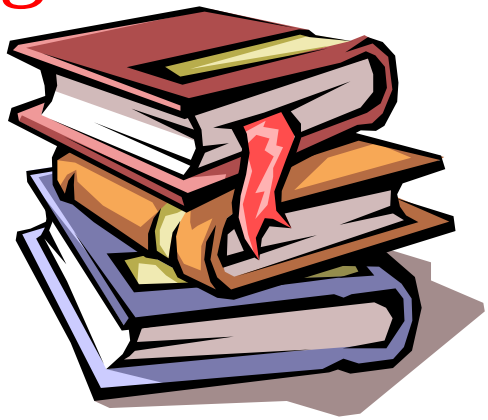
Digital Signatures

Lecture Contents

- Section-1:Digital Signatures
- Section-2:Encryption and Decryption
- Section-3:Private Key Protection
- Section-4:Public key Infrastructure
- Section-5:Summary and E-Goverence

Electronic Record

1. Very easy to make copies
2. Very fast distribution
3. Easy archiving and retrieval
4. Copies are as good as original
5. Easily modifiable
6. Environmental Friendly



Because of 4 & 5 together, these lack authenticity

Why Digital Signatures?

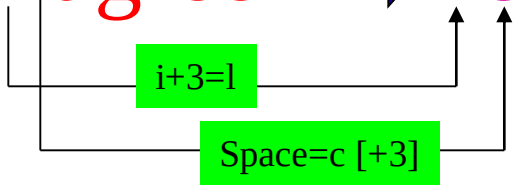
- To provide Authenticity, Integrity and Non-repudiation to electronic documents
- To use the Internet as the safe and secure medium for e-Commerce and e-Governance

Encryption

Caesar Cipher

The shift is linear and equidistributed 3 changes

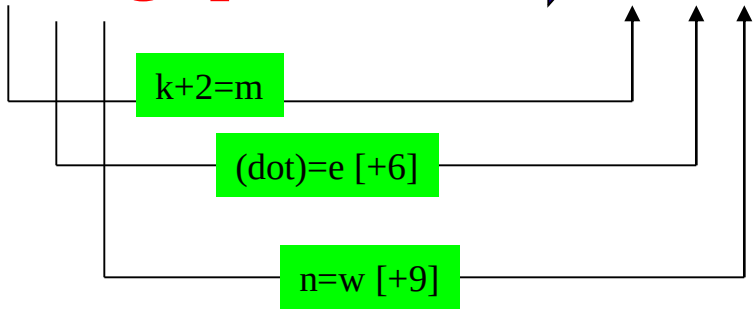
I agree ⇒ lcdjuhh



Key Cipher

The shift is linear (cyclic) 269

k.n.gupta 62 ⇒ mewam3rzjba



Char	1	2	3	4	5	6	7	8	9
a	b	c	d	e	f	g	h	i	j
b	c	d	e	f	g	h	i	j	k
c	d	e	f	g	h	i	j	k	l
d	e	f	g	h	i	j	k	l	m
e	f	g	h	i	j	k	l	m	n
f	g	h	i	j	k	l	m	n	o
g	h	i	j	k	l	m	n	o	p
h	i	j	k	l	m	n	o	p	q
i	j	k	l	m	n	o	p	q	r
j	k	l	m	n	o	p	q	r	s
k	l	m	n	o	p	q	r	s	t
l	m	n	o	p	q	r	s	t	u
m	n	o	p	q	r	s	t	u	v
n	o	p	q	r	s	t	u	v	w
o	p	q	r	s	t	u	v	w	x
p	q	r	s	t	u	v	w	x	y
q	r	s	t	u	v	w	x	y	z
r	s	t	u	v	w	x	y	z	0
s	t	u	v	w	x	y	z	0	1
t	u	v	w	x	y	z	0	1	2
u	v	w	x	y	z	0	1	2	3
v	w	x	y	z	0	1	2	3	4
w	x	y	z	0	1	2	3	4	5
x	y	z	0	1	2	3	4	5	6
y	z	0	1	2	3	4	5	6	7
z	0	1	2	3	4	5	6	7	8
0	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	.
2	3	4	5	6	7	8	9	.	
3	4	5	6	7	8	9	.		a
4	5	6	7	8	9	.		a	b
5	6	7	8	9	.		a	b	c
6	7	8	9	.		a	b	c	d
7	8	9	.		a	b	c	d	e
8	9	.		a	b	c	d	e	f
9	.		a	b	c	d	e	f	g
. (Dot)		a	b	c	d	e	f	g	h
Space	a	b	c	d	e	f	g	h	i

ENCRYPTION

Message 1

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

Encrypted Message 1

9a46894335be49f0b9cab28d755aaa9cd985
71b275bbb0adb405e6931e856ca3e5e569e
dd135285482

Same Key
SYMMETRIC

Message 2

The Internet knows no ge
It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

Encrypted Message 2

a520eecb61a770f947ca856cd675463f1c95
a9a[illegible]71f80830c87f5715f5f593349
8dd7e[illegible]
67c3[illegible]

Different Keys
[Keys of a pair – Public and Private]
ASYMMETRIC
[PKI]

DECRYPTION

Encrypted Message 1

9a46894335be49f0b9cab28d755aaa9cd98571b
275bbb0adb405e6931e856ca3e5e569edd13528
5482

Message 1

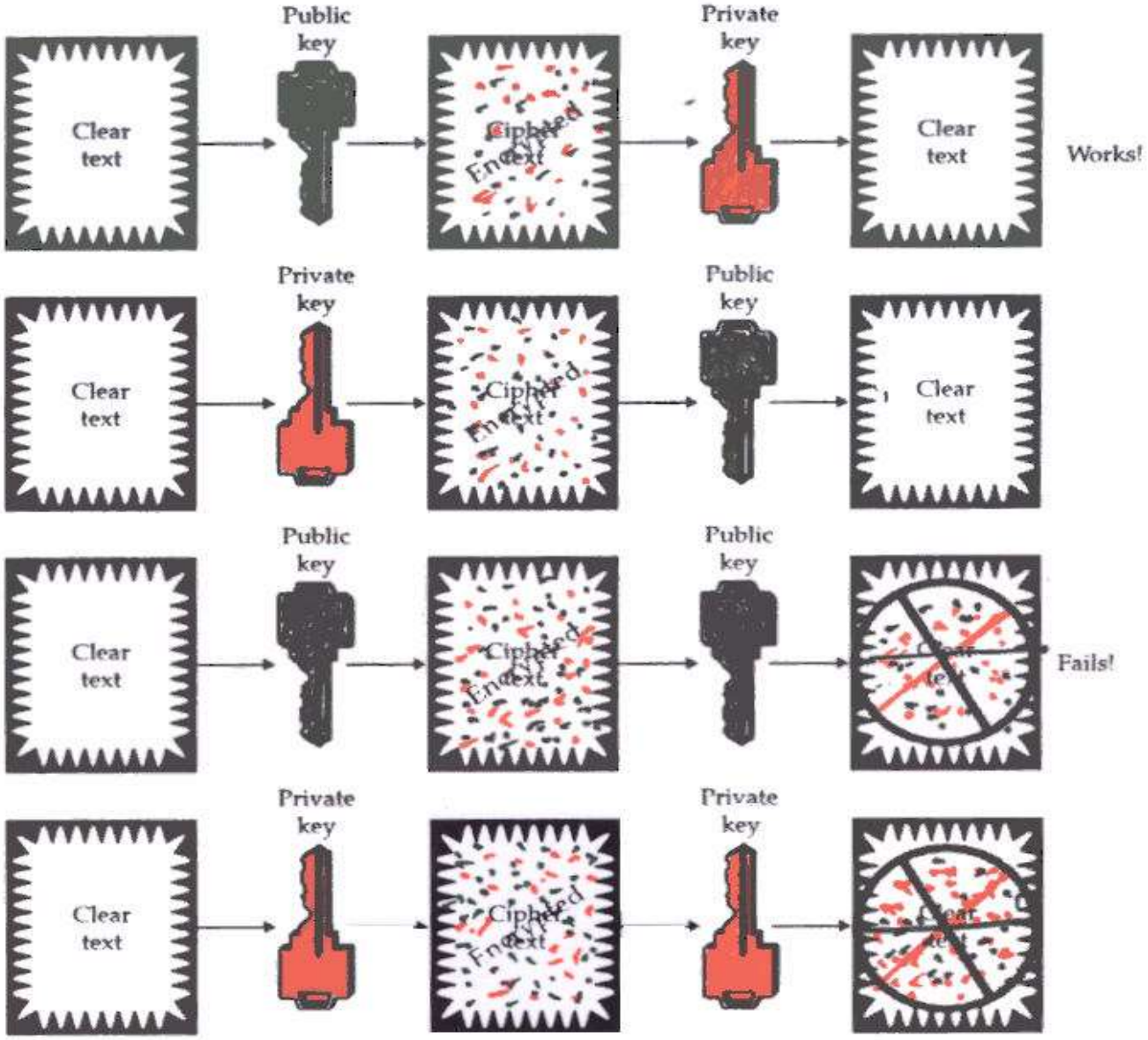
Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

Encrypted Message 2

a520eecb61a770f947ca856cd675463f1c95a9a2b
8d4e6a71f80830c87f5715f5f59334978dd7e97da
0707b48a1138d77ced56feba2b467c398683c7db
eb86b854f120606a7ae1ed934f5703672adab0d7
be66dccde1a763c736cb9001d0731d541106f50b
b7e54240c40ba780b7a553bea570b99c9ab3df13
d75f8ccfdddeaaf3a749fd1411

Message 2

The Internet knows no geographical boundaries. It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.


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 Signatures

I agree

efcc61c1c03db8d8ea8569545c073c814a0ed755

My place of birth is at Gwalior.

fe1188eecd44ee23e13c4b6655edc8cd5cdb6f25

I am 62 years old.

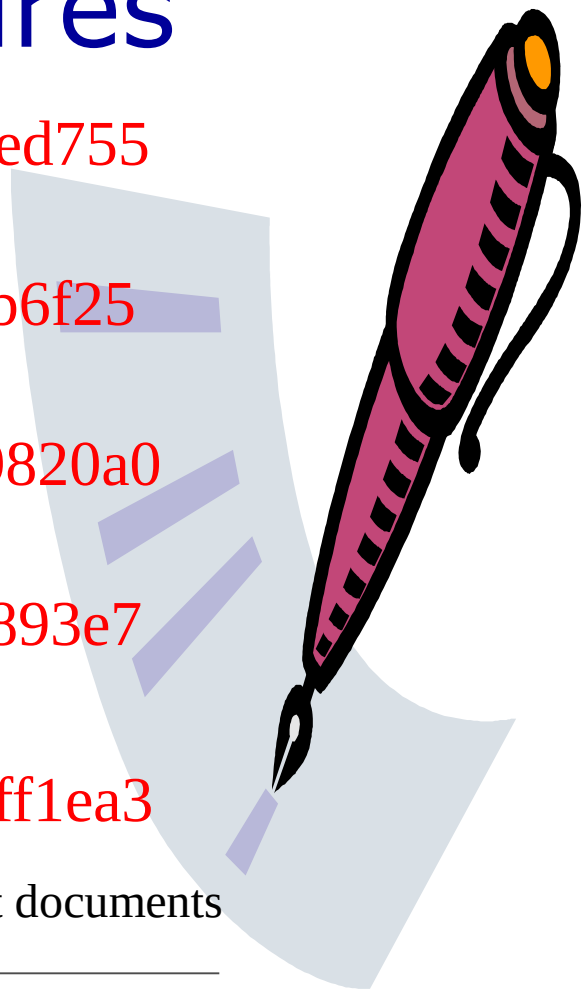
0e6d7d56c4520756f59235b6ae981cdb5f9820a0

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 document content dependent

Concepts

- **A 1024 bits number is a very big number much bigger than the total number of electrons in whole world.**
- **Trillions of Trillions of pairs of numbers exist in this range with each pair having following property**
  - **A message encrypted with one element of the pair can be decrypted ONLY by the other element of the same pair**
- **Two numbers of a pair are called keys, the Public Key & the Private Key. User himself generates his own key pair on his computer**

- **Any message irrespective of its length can be compressed or abridged uniquely into a smaller length message called the Digest or the Hash.**
- **Smallest change in the message will change the Hash value**

Click for Hash Generation

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**

Digital Signatures

Each individual generates his own key pair
[Public key known to everyone & Private key only to the owner]

Private Key – Used for making digital signature

Public Key – Used to verify the digital signature

RSA Key pair

(including Algorithm identifier)

[2048 bit]

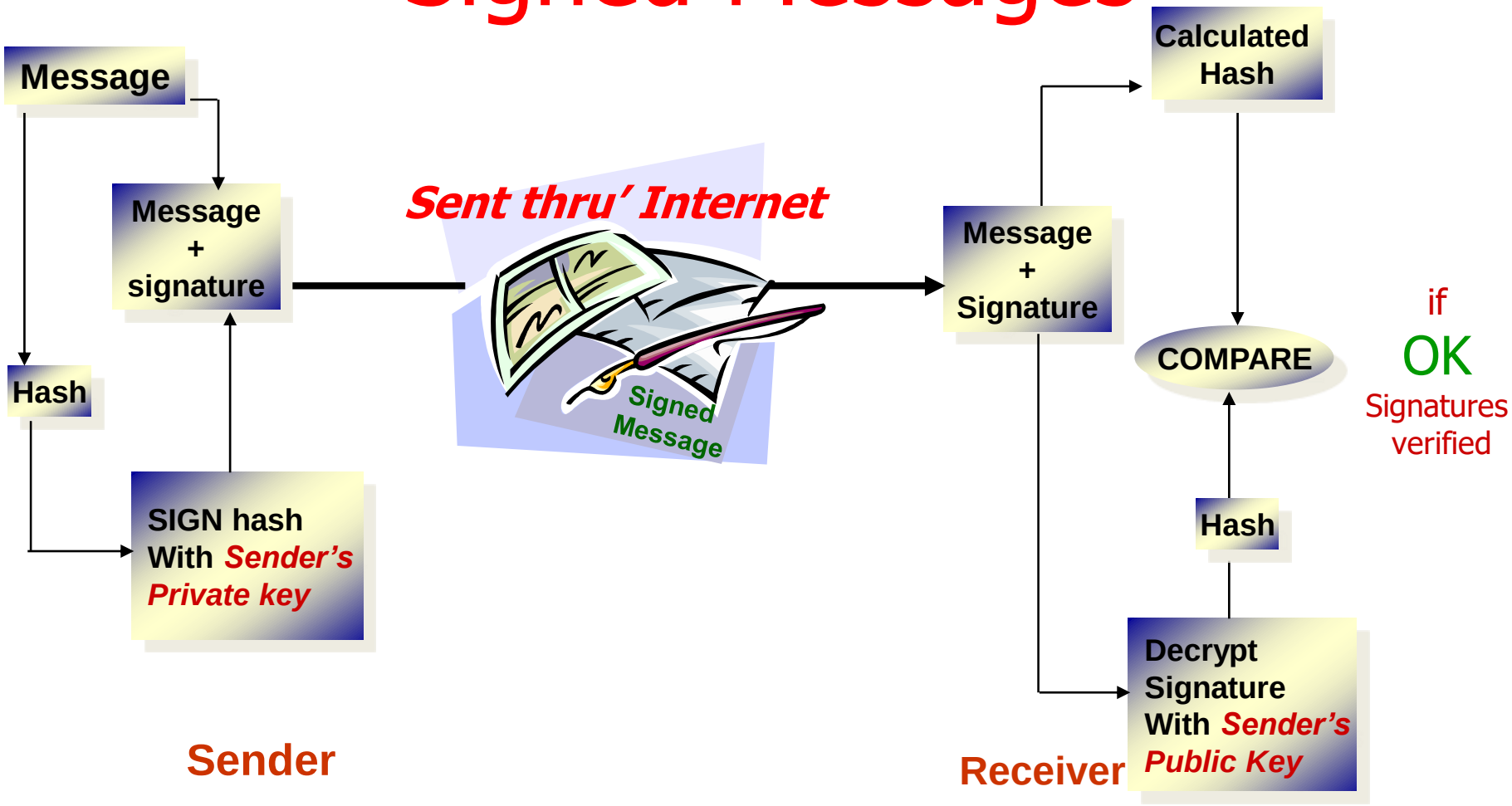
Private Key

```
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
```

Signed Messages

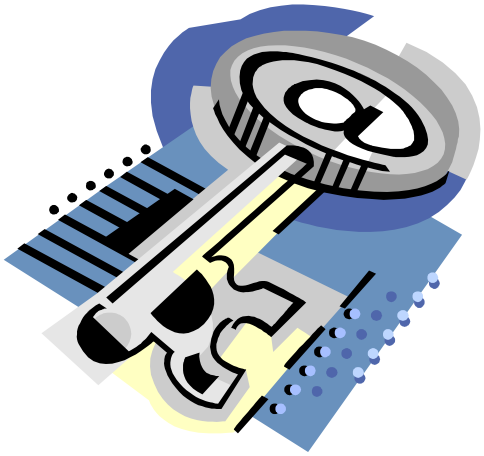


Paper signatures v/s Digital Signatures

V/s

Parameter	Paper	Electronic
Authenticity	May be forged	Can not be copied
Integrity	Signature independent of the document	Signature depends on the contents of the document
Non-repudiation	a. Handwriting expert needed b. Error prone	a. Any computer user b. Error free

Key points



- **Key Generation**
  - Random Numbers
  - RSA Key Pair [Private/Public Key]
- **Digital Signature**
  - Generate Message Digest [SHA1]
  - Encrypting Digest using Private Key [Signatures]
  - Attaching the Signatures to the message.
- **Verification of Signatures**
  - Run the test for Authentication, Integrity and Non repudiation.
- **Digital Signature Certificate**
  - ITU X.509 v3

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 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 also not preferred because**
  - **The key becomes static and machine dependent.**
  - **The key is in known file format.**

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

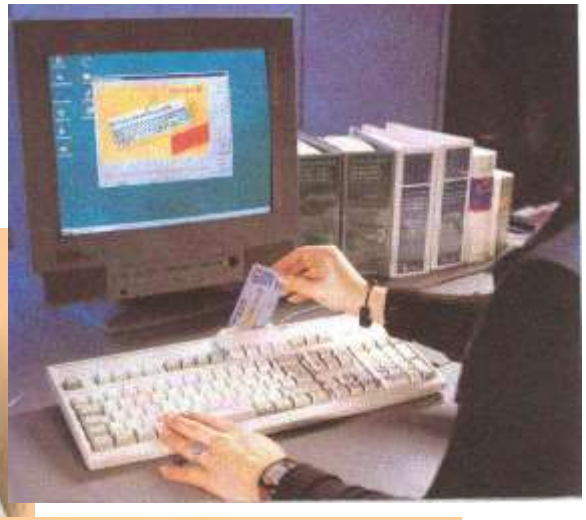
- **They are similar to smart cards in functionality as**
  - **Key is generated inside the token.**
  - **Key is highly secured as it doesn't leave the token.**
  - **Highly portable.**
  - **Machine Independent.**
- **iKEY is one of the most commonly used token as it doesn't need a special reader and can be connected to the system using USB port.**

Hardware Tokens

iKey

Smart Card

Biometrics – adds another level of security to these tokens




WindowsNT

Public Key Infrastructure (PKI)

- Some Trusted Agency is required which certifies the association of an individual with the key pair.

  Certifying Authority (CA)

- This association is done by issuing a certificate to the user by the CA

  Public key certificate (PKC)

- All public key certificates are digitally signed by the CA

Certifying Authority

- Must be widely known and trusted
- Must have well defined Identification process before issuing the certificate
- Provides online access to all the certificates issued
- Provides online access to the list of certificates revoked
- Displays online the license issued by the Controller
- Displays online approved Certification Practice Statement (CPS)
- Must adhere to IT Act/Rules/Regulations and Guidelines

IDRBT Certificate

Paper

क्र. सं./No. 2002 0003 050807 000 0000 999

भारत सरकार
GOVERNMENT OF INDIA
प्रमाणन प्राधिकारी नियंत्रक
CONTROLLER OF CERTIFYING AUTHORITIES

प्रमाणित किया जाता है कि बैंकिंग प्रौद्योगिकी विकास एवं अनुसंधान संस्थान
स्थापना स्थल कैसल हिल्स, रोड नं: १, मासब टैंक, हैदराबाद - ५०००५७.
को सूचना प्रौद्योगिकी अधिनियम 2000 के अधीन, 9 जुलाई, 2001 को जारी विनियमों के भाग के रूप में विहित निबंधनों एवं शर्तों के अध्यधीन, सूचना प्रौद्योगिकी अधिनियम 2000 की धारा 21 के अन्तर्गत, प्रमाणन प्राधिकारी के रूप में कार्य करने के लिए लाइसेंस प्रदान किया गया है। यह लाइसेंस आज दिनांक 6 माह अगस्त, २००२ को प्रमाणन प्राधिकारी के नियंत्रक के हस्ताक्षर एवं मुहर सहित जारी किया जाता है, और लाइसेंस की सम्पूर्ण वैधता अवधि के दौरान सूचना प्रौद्योगिकी अधिनियम, नियम, विनियम और दिशा-निर्देशों के अनुपालन के अध्यधीन यह पाँच वर्षों की अवधि के लिए वैध है।

This is to certify that INSTITUTE FOR DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY
located at CASTLE HILLS, ROAD NO.1, MASAB TANK, HYDERABAD - 500 057.
has been granted licence to act as a Certifying Authority, under Section 21 of the IT Act 2000, subject to Terms and Conditions specified as part of the Regulations dated 9th July, 2001, issued under the IT Act 2000. This licence is given under the signature and seal of the Controller of Certifying Authorities on this 6th *day of* August, 2002, *and is valid for a period of five years, subject to compliance with the IT Act, Rules, Regulations and Guidelines during the entire validity of the licence.*

Debjani Nag
DEBJANI NAG
Assistant Controller (Tech.)
Office of Controller of Certifying Authorities
Department of Information Technology
Government of India
Electronics Niketan
6, C.G.O. Complex, New Delhi-3
Tel: 4366804
प्राधिकृत/Authorised हस्ताक्षरकर्ता/Signatory

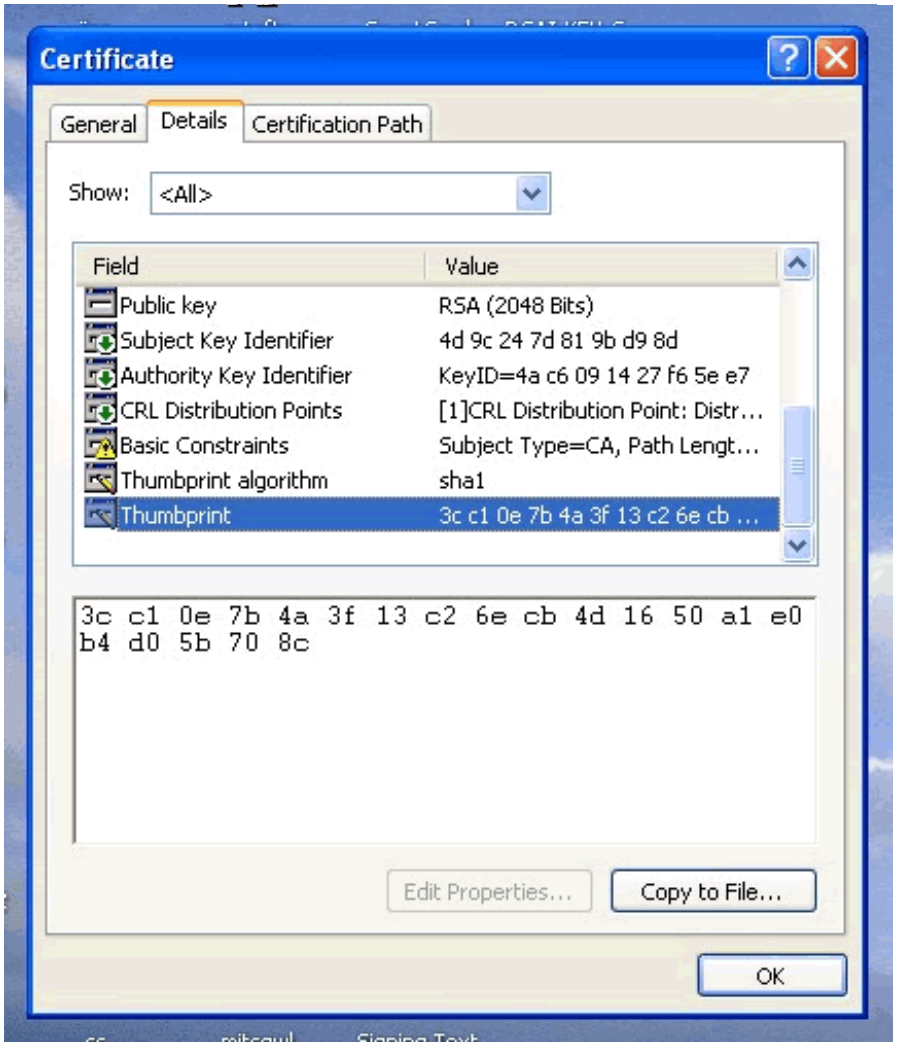
LOVI RAJ GUPTA
Assistant Controller (Tech.)
Office of Controller of Certifying Authorities
Department of Information Technology
Government of India
Electronics Niketan
6, C.G.O. Complex, New Delhi-3

सार्वजनिक कुंजी
Public Key

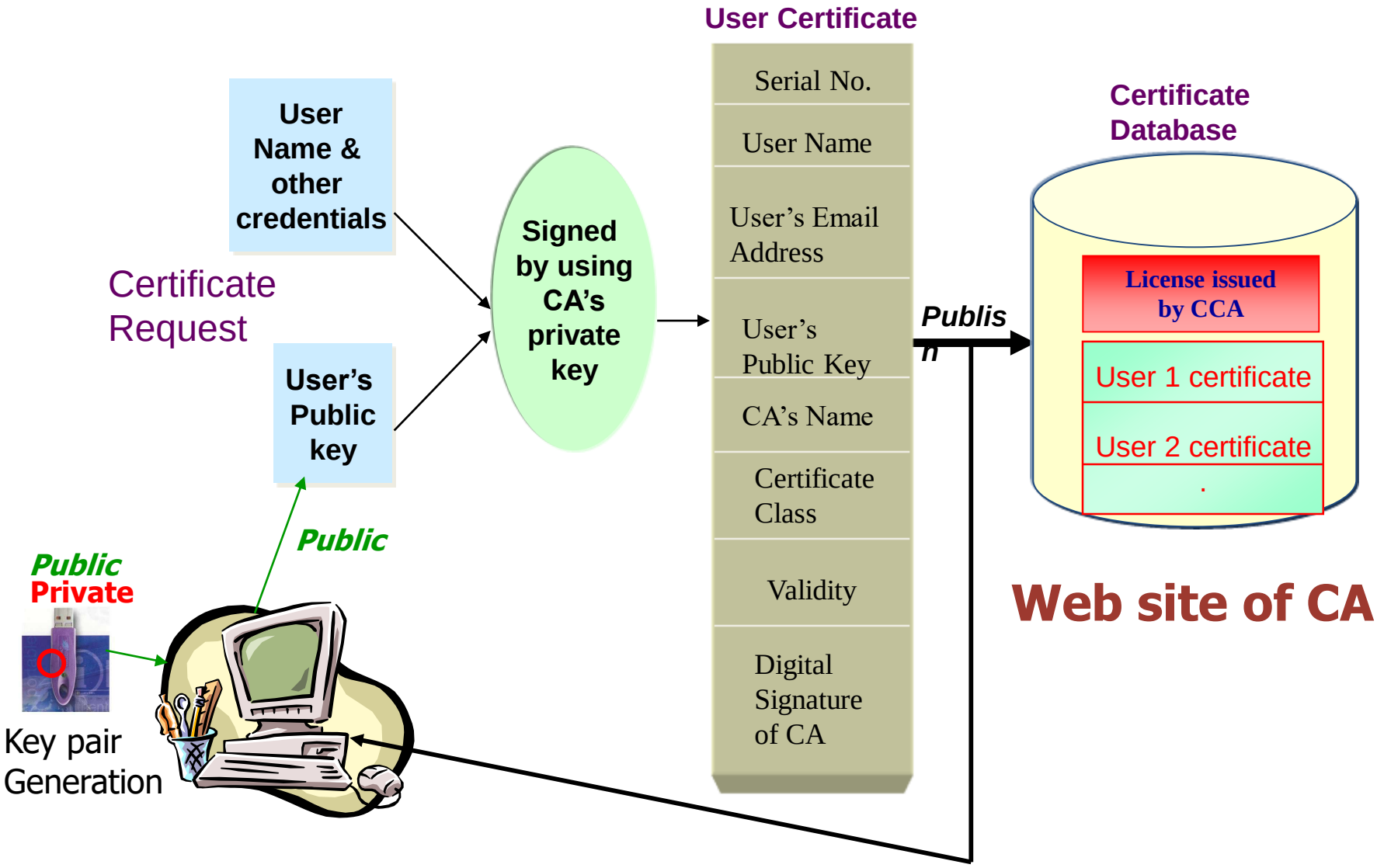
```
3082 010a 0282 0101 00d2 8269 d5f3 270d 5271 0daf 77a7 ad17 2c6c 8293 bc6d d90e 2b71 7788 e0b8 bef9 3b6c
6e15 f00a 33a6 8f78 78bd 81c9 a6df f067 3791 e55a a378 f2a3 d14e 8bf0 2e15 d541 b70c 3964 5954 7b45 2e1a
109b f8e9 5ed4 c17b c57b 2364 d0c5 4536 bc9f 78d7 ee37 0ffa 9952 feb5 5656 8866 6a00 9fb4 8960 d95c 4687
1840 c38b 33ac 64b3 be95 786b 211f 3cc4 b257 641e 8320 457b 9d5d 6295 f7c6 87de 9680 af5c bb50 bc49 1f89
023a 6b2e 6bfd baed b6a3 f94d b893 5240 20e3 7b85 a939 45d9 56b1 da46 9b3b c174 7cd0 86fc 19c0 f72a b4e4
8f4c 6dcb e7a4 8c4c 2486 abad 9f4b f385 7512 e138 1bd1 ab81 716e dd08 7010 7ee3 83f3 8adc 7783 1249 2c4a
21b8 eba6 1748 5724 2e88 305f 8902 0301 0001
```

Debjani Nag

Electronic



Public-Key Certification

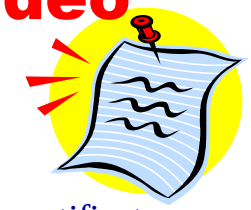


Private key of CA or CCA require highest level of security

Hardware Security Module (HSM) is used for storing the Private Key

More than one person are required for signing

HSM is housed in a strong room with video surveillance on 24x7 basis.



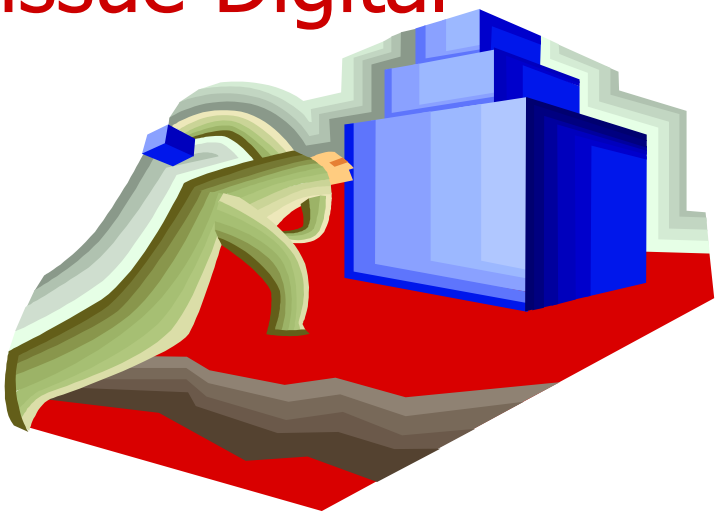
Click for certificate generation demo

Trust Path

- Controller is the Root certifying authority responsible for regulating Certifying Authorities (CAs)
- Controller certifies the association of CA with his public key
- Certifying Authority (CA) is the trusted authority responsible for creating or certifying identities.
- CA certifies the association of an individual with his public key

Role of controller

Controller of Certifying Authorities as the "Root" Authority certifies the technologies,infrastructure and practices of all the Certifying Authorities licensed to issue Digital Signature Certificates



Summary

- Each individual has a pair of keys
- Public key of each individual is certified by a CA (Certifying Authority)
- Public keys of CAs are certified by the Controller
- Public key of the Controller is self certified
- Public keys of everyone are known to all concerned and are also available on the web
- Certification Practice Statement is displayed on the web site

Applications in Judiciary

1. Instant posting of judgment on the web.
2. Secured electronic communications within judiciary
3. Authentic archiving of Judicial records
4. Submission of affidavits
5. Giving certified copies of the Judgment

Applications in Telecommunications

A. Subscribers

- Subscriber's services management
  - STD/ISD, Opening, Closing, Initializing Password
- Shifting of telephones, Accessories (Clip, Cordless)
- Small Payments through telephones bills
  - Books, gifts, Internet purchases
- Mobile Authentication of SMS
  - Share market trading, Intra/Inter office instructions
- Mobile Phones as Credit cards
  - Mobile operator can venture into credit card business

Applications in Telecommunications *(contd.)*

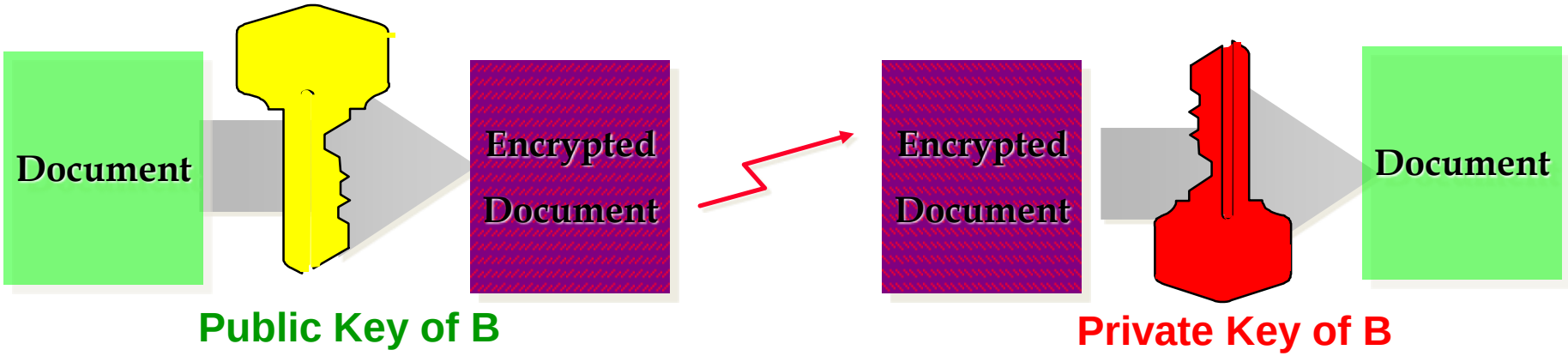
B. Internal

- Intra/Inter offices authentic communications
  - OBs, approvals, Instructions, requests
- Procurement of material
  - Calling/Receiving bids, Purchase orders, Payment instructions
- Network Management functions
  - Change of configuration, Blocking/unblocking routes

Public Key Cryptography

Encryption Technologies

Confidentiality



E-Governance

- Empowering Citizens
  a) Transparency
  b) Accountability
  c) Elimination of Intermediatory
  d) Encouraging Citizens to exercise their Rights

Government Online

1. Issuing forms and licences
2. Filing tax returns online
3. Online Government orders/treasury orders
4. Registration
5. Online file movement system
6. Public information records
7. E-voting
8. Railway reservations & ticketing
9. E-education
10. Online money orders

Thank You