Admissibility of Electronic Record

Bhartiya Sakshya Adhiniyam, 2023

Sec. 2. (1) (d) BSA:

"document" means any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or any other means or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter and **includes electronic and digital records.**

Bhartiya Sakshya Adhiniyam, 2023

Sec. 2. (1) (e) BSA:

"evidence" means and includes—

(i) all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence;

(ii) all documents including **electronic or digital records** produced for the inspection of the Court and such documents are called documentary evidence;

Bharatiya Nyaya Sanhita, 2023

Sec. 2. (8) BNS:

"document" means any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, and **includes electronic and digital record**, intended to be used, or which may be used, as evidence of that matter.

Sec. 2 (1) (d) BSA: "document", adds "**electronic and digital records**" within its ambit.

Illustrations (vi)

✓An electronic record on emails

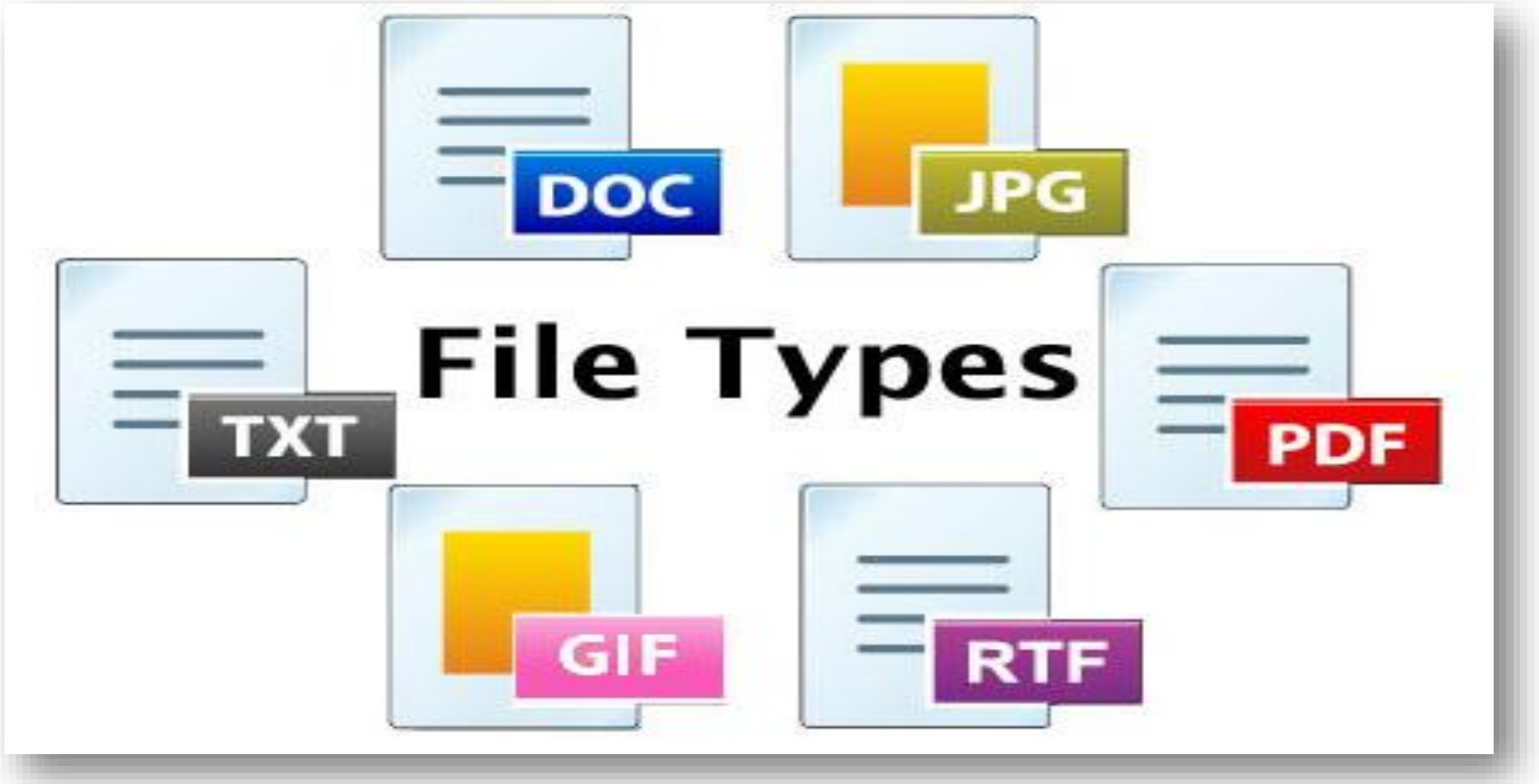
✓server logs

You will find user's IP address along with the timestamp and date

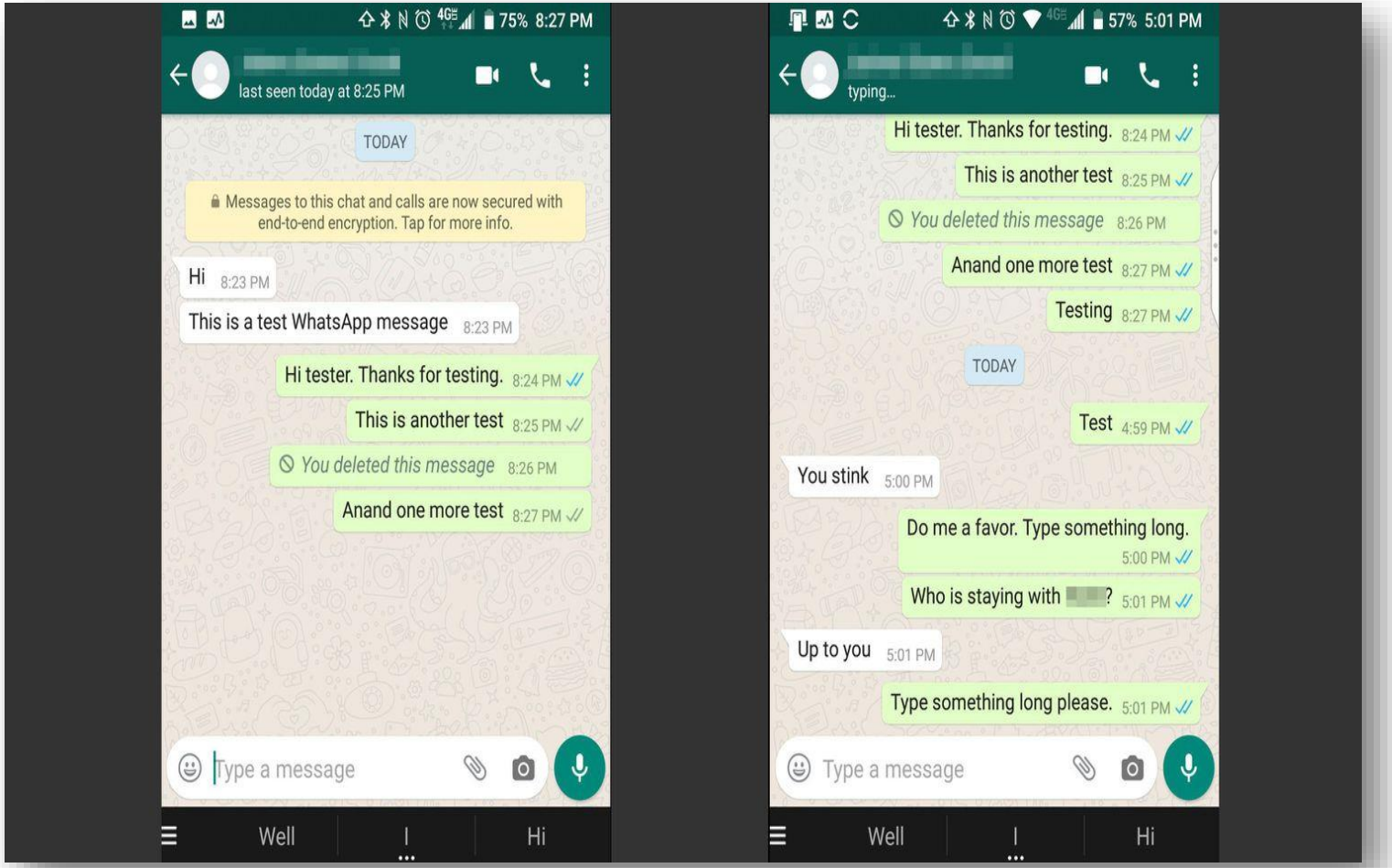
```
root@ubuntu:/var/log/apache2# cat access.log

192.168.0.104 - - [29/Aug/2017:10:04:59 -0700] "GET /dvwa HTTP/1.1" 301 574 "-" "Mozilla/5.0 (Windows NT 10.0; Win6
HTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:04:59 -0700] "GET /dvwa/ HTTP/1.1" 302 553 "-" "Mozilla/5.0 (Windows NT 10.0; Wir
KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:04:59 -0700] "GET /dvwa/login.php HTTP/1.1" 200 1086 "-" "Mozilla/5.0 (Windows NT
t/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:00 -0700] "GET /dvwa/dvwa/css/login.css HTTP/1.1" 200 740 "http://192.168.0.10
0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:00 -0700] "GET /dvwa/dvwa/images/login_logo.png HTTP/1.1" 200 9374 "http://192
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:00 -0700] "GET /favicon.ico HTTP/1.1" 404 502 "http://192.168.0.102/dvwa/login
T 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP HTTP/1.1" 301 576 "-" "Mozilla/5.0 (Windows NT 10.0; Win
KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP/ HTTP/1.1" 302 248 "-" "Mozilla/5.0 (Windows NT 10.0; Wi
(KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP/portal.php HTTP/1.1" 302 384 "-" "Mozilla/5.0 (Windows N
it/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP/login.php HTTP/1.1" 200 1783 "-" "Mozilla/5.0 (Windows N
it/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP/stylesheets/stylesheet.css HTTP/1.1" 200 2088 "http://19
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.3
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP/images/owasp.png HTTP/1.1" 200 17274 "http://192.168.0.1
5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP/images/zap.png HTTP/1.1" 200 17843 "http://192.168.0.102
0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP/images/netsparker.png HTTP/1.1" 200 2173 "http://192.168
lla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP/images/mk.png HTTP/1.1" 200 11512 "http://192.168.0.102/
```

✓**documents on computers, laptop or smartphone**



✓Messages


75% 8:27 PM
last seen today at 8:25 PM
TODAY
Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.
Hi 8:23 PM
This is a test WhatsApp message 8:23 PM
Hi tester. Thanks for testing. 8:24 PM
This is another test 8:25 PM
You deleted this message 8:26 PM
Anand one more test 8:27 PM
Type a message
Well
I
Hi
57% 5:01 PM
typing...
Hi tester. Thanks for testing. 8:24 PM
This is another test 8:25 PM
You deleted this message 8:26 PM
Anand one more test 8:27 PM
Testing 8:27 PM
TODAY
Test 4:59 PM
You stink 5:00 PM
Do me a favor. Type something long. 5:00 PM
Who is staying with ? 5:01 PM
Up to you 5:01 PM
Type something long please. 5:01 PM
Type a message
Well
I
Hi

✓Websites

✓locational evidence

✓voice mail messages stored on digital devices are documents;

Bhartiya Sakshya Adhiniyam, 2023

Sec. 57 BSA:

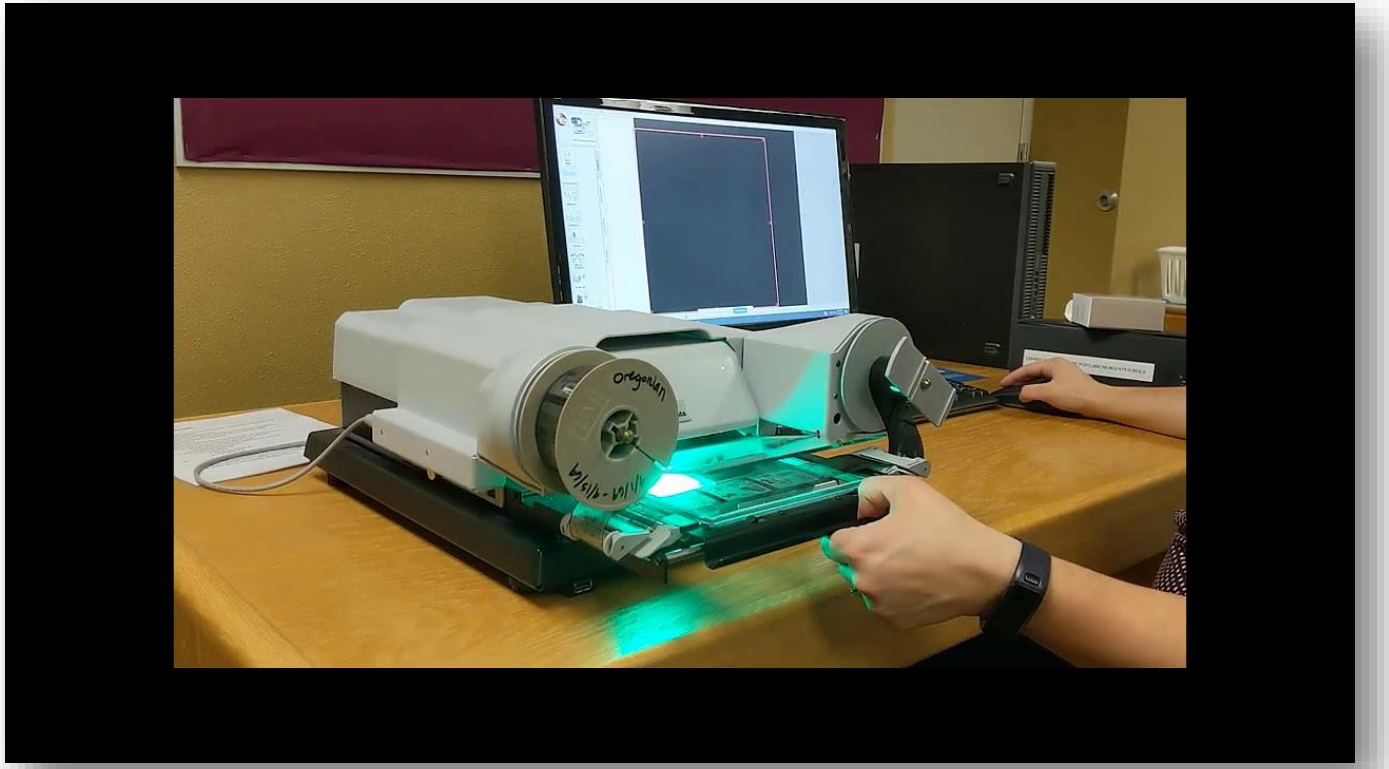
Electronic records & Digital Records will also be considered as documents & classifies as **primary evidence**. Primary evidence includes the original document and its parts, such as electronic records and video recordings.

Sec. 61 BSA:

The said Section clearly states that any electronic/digital record shall have the **'same legal effect, validity and enforceability as other document'** and its admissibility cannot be denied merely on the ground that it is electronic/digital record.

The BSA provides that **electronic or digital records will have the same legal effect as paper records**.

[Sec. 61 BSA]



Electronic Record

Section 2(1) (t) in The Information Technology Act, 2000

"electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

Electronic records are those that are **created and exist exclusively within computer systems**.

Example:

- Emails and attachments
- Websites
- Databases
- Spreadsheets / Excel Files
- Software Applications
- Web Pages and Blogs
- Text messages
- Social Media Postings
- Word documents
- Images
- Videos and audio files

Digital records refer to either **digitized versions of physical documents or documents originally created in a digital environment**. To read and understood the digital record, combination of computer hardware and software is required.

Example:

- Scanned Documents
- Photographs
- Digital Audio and Video Files
- E-books and PDFs

Sec. 2 (1) (o) of IT Act: data

"data" means a representation of

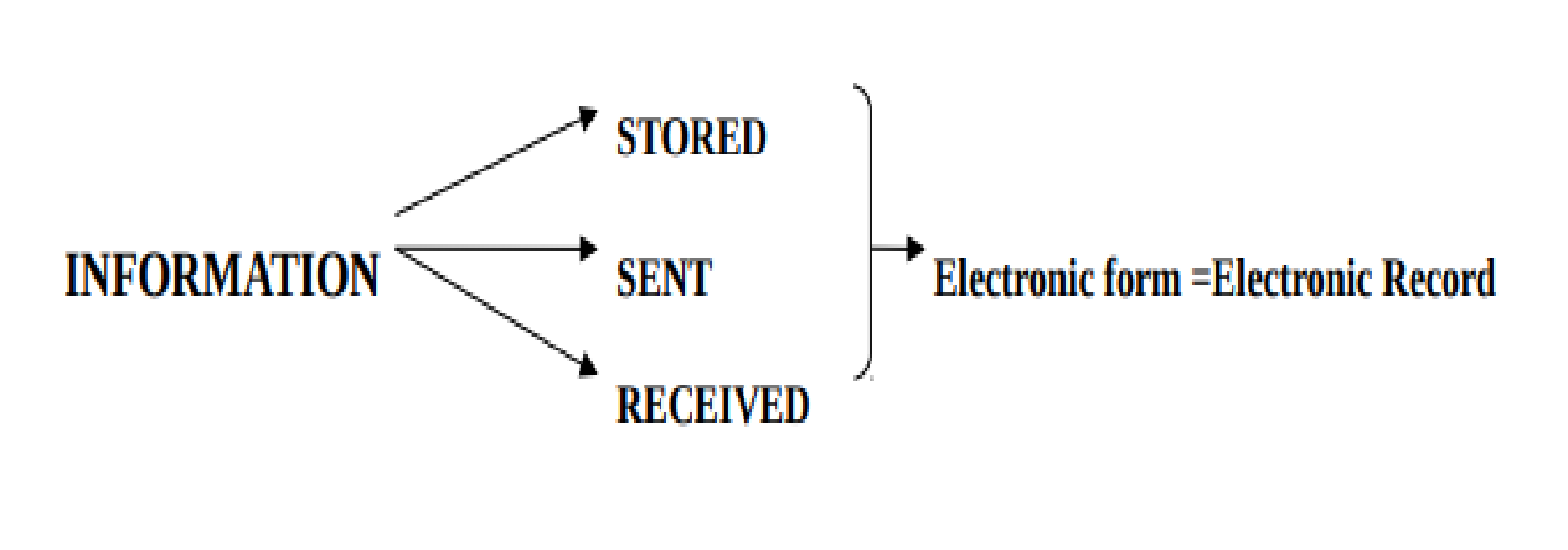
- information,
- knowledge,
- facts,
- concepts or instructions
- which are being prepared or have been prepared in a formalised manner, and
- is intended to be processed, is being processed or has been processed in a computer system or computer network, and
- may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

Sec. 2 (1) (r) of IT Act: electronic form

"electronic form" with reference to information, means any information

- generated,
- sent,
- received or
- stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

Thus, if any information is **stored, sent or received in electronic form**, it is termed as electronic record.



Sec. 3: Authentication of electronic records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his **digital signature**.

(2) The authentication of the electronic record shall be effected by the use of **asymmetric crypto system** and **hash function** which envelop and transform the initial electronic record into another electronic record.

Explanation.–For the purposes of this sub-section, –hash function means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as –hash result such that **an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible**–

(a)to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b)that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Sec. 4: Legal recognition of electronic records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is–

(a) rendered or made available in an electronic form; and (b) accessible so as to be usable for a subsequent reference.

Asymmetric Cryptography (Public Key Cryptography)

Asymmetric Cryptography, also known as public key cryptography, uses **public and private keys** to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

Sec. 2 (1) (f) of IT Act: Asymmetric Crypto System

"asymmetric crypto system" means a system of a **secure key pair** consisting of a **private key** for creating a digital signature and a **public key** to verify the digital signature.

Sec. 2 (1) (x): key pair

"key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

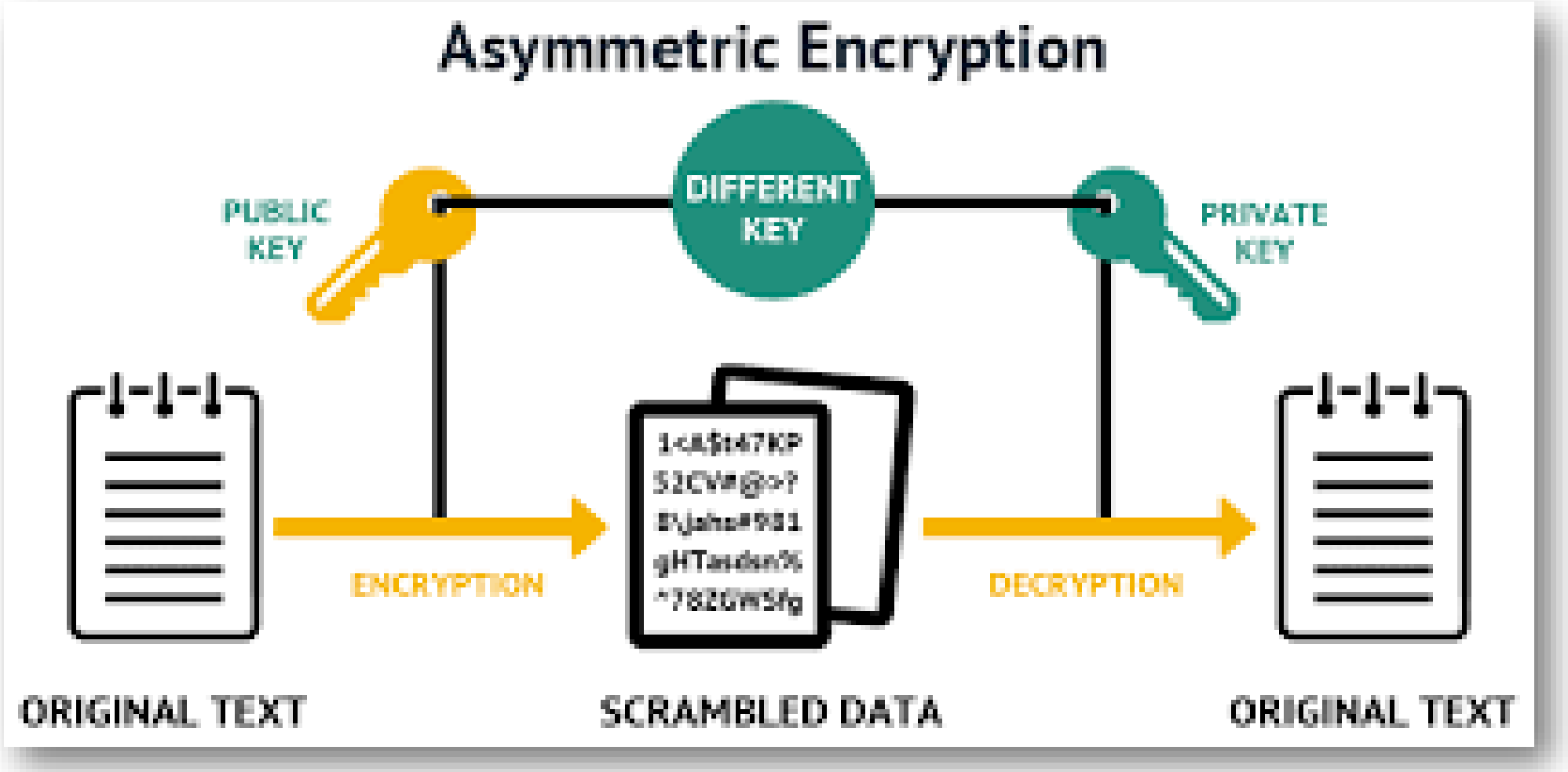
Sec. 2 (1) (zc): private key

"private key" means the key of a key pair used to create a digital signature.

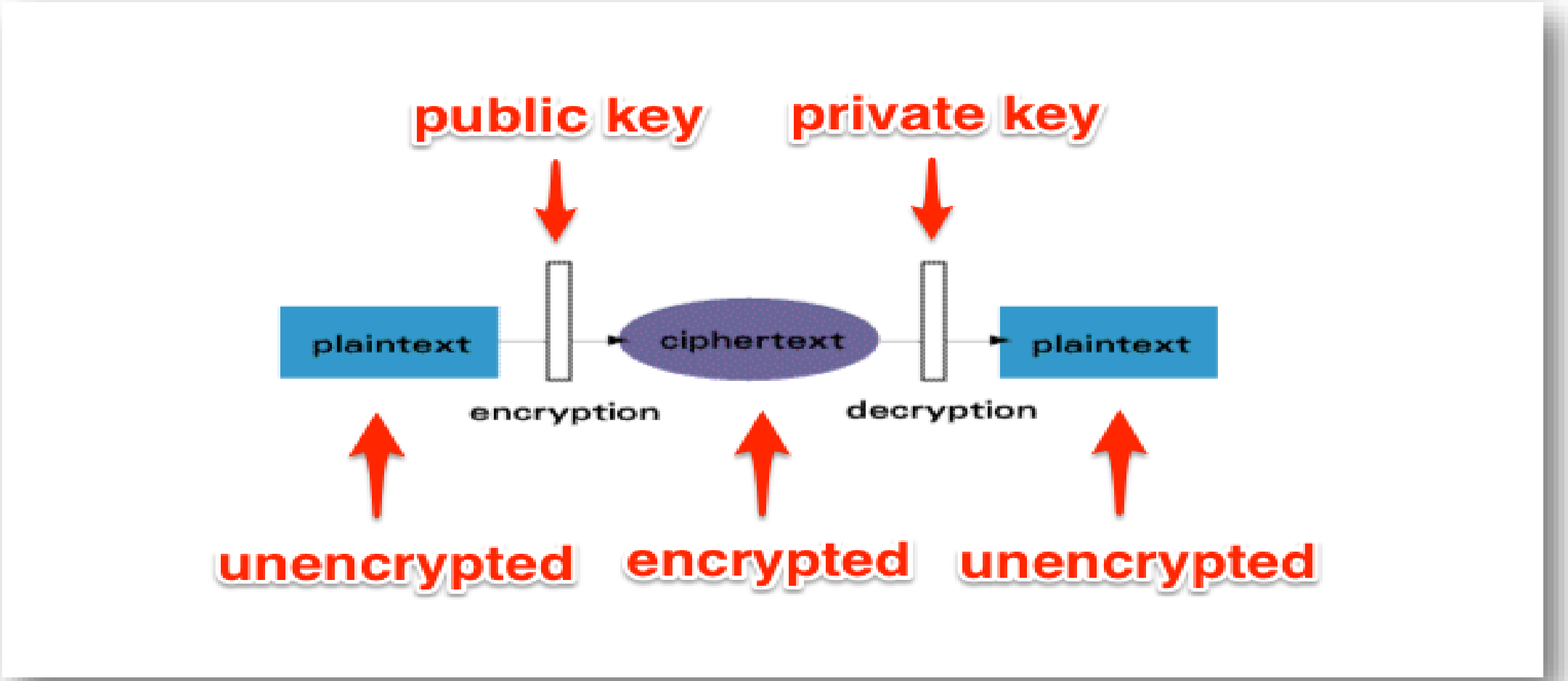
Sec. 2 (1) (zd): public key

"public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

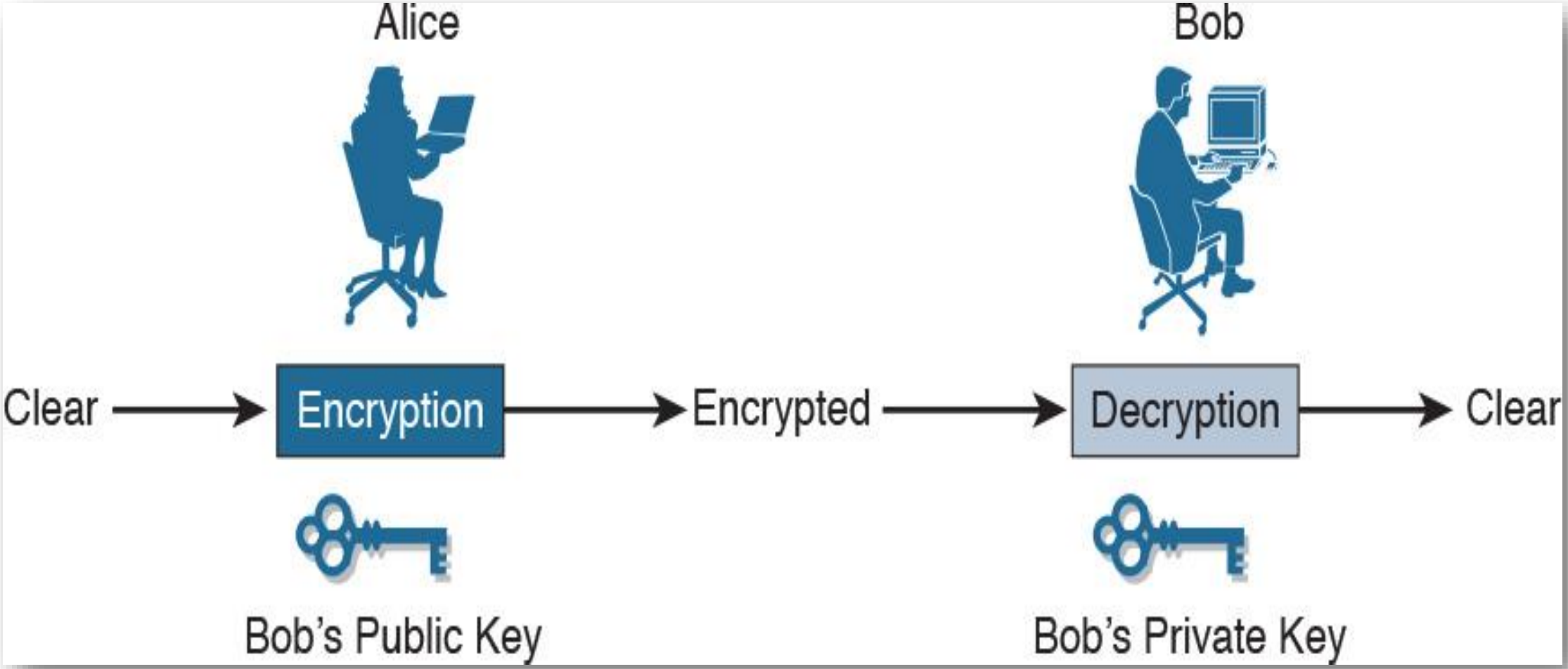
Asymmetric Cryptography (Public Key Cryptography)



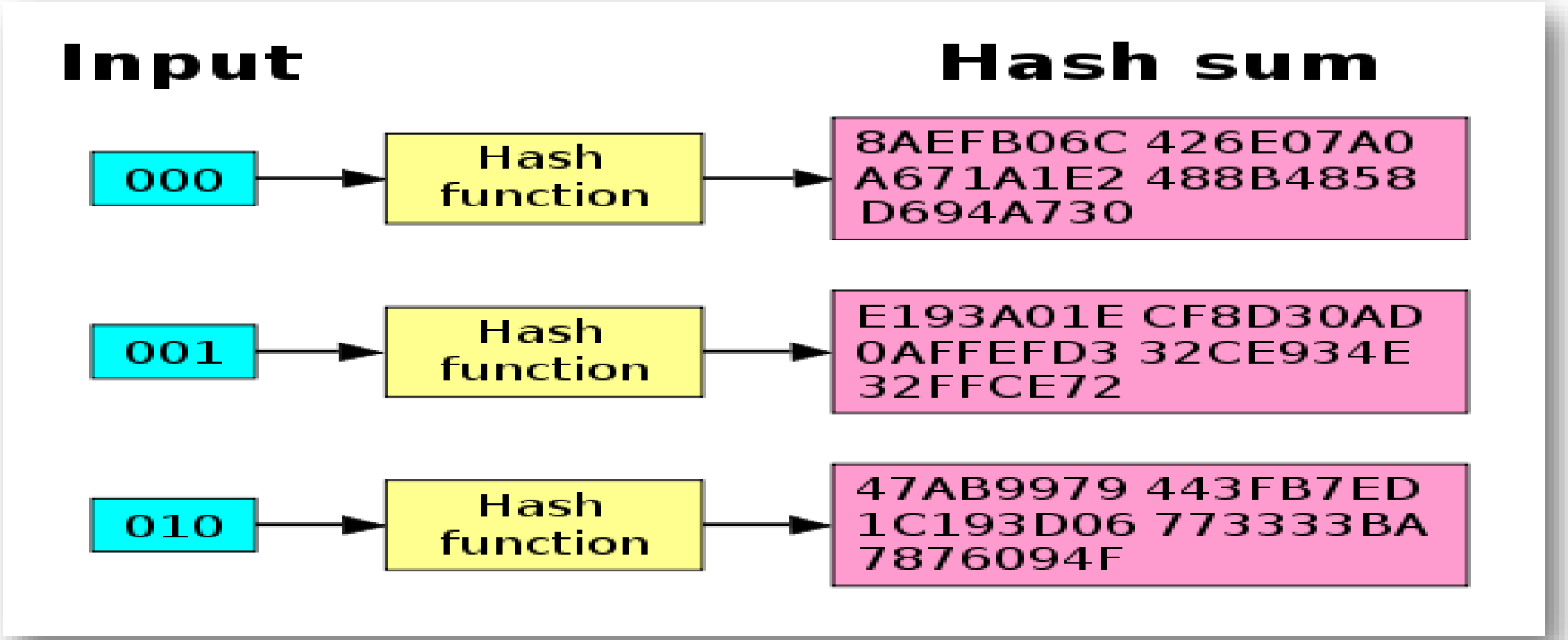
Asymmetric Cryptography (Public Key Cryptography)



Asymmetric Cryptography (Public Key Cryptography)



Hash Function



What are Hash Function?

- A hash function is a mathematical algorithm that converts any data into a fixed-length string of characters, called a hash value.
- A Hash Value (also called as Hashes or Checksum) is a string value (of specific length), which is the result of calculation of a Hashing Algorithm.
- To determine the Integrity and authenticity of any Data (which can be a file, folder, email, attachments, downloads etc), Hash Function is necessary.
- **Hashing is a Fingerprinting or Thumb Print of any digital data.**
- The most wonderful character of Hash Value is that they are highly unique.
- **No two data can theoretically have same Hash Value.**

Features:

- The **hash value size is permanently fixed**, and it's independent of the input data size.
- You can use hashing in cryptographic applications **like a digital signature**.
- **Two different input files cannot produce the same hash value.**
- **Hash values don't depend on the name of the file**. Even if the file names are different and their contents are identical, it will produce the same hash values corresponding to these files.

Features:

- Hashing algorithms are **one-way functions** — **you can't figure out the original input data using the hash value**.
- **The output length of all hashing algorithms should be the same, regardless of the length of the input size**.
- Different hash functions will produce different hash values corresponding to the same contents in the respective files.

- **Hashing is a one-way function or process.**

What this means is that once an input gets hashed, there's no way back. It's one of the things that make hashes so unique.

- **Encryption, on the other hand, is a two-way method.**

This is an entirely different process that can't be reversed or decrypted (because there's nothing to decrypt). It means that when something is encrypted, it's supposed to be decrypted, meaning it's essentially reverted to its original form.

Hashing Algorithm

Plain Text

Hash Function

Hashed Text

Encryption & Decryption

Plain Text

Encryption

Encrypted Text

Decryption

Plain Text

Different popular hashing algorithms:

- **MD5** (Message Digest 5) - once widely used but now considered less secure due to potential collisions.
- **SHA-1** (Secure Hashing Algorithm 1) also facing security concerns and phasing out.
- **SHA-2** (Secure Hashing Algorithm 2) family (SHA-256, SHA-384, SHA-512)- widely used, secure, and recommended for most applications.
- **SHA-3** (Secure Hashing Algorithm 3) - newer, more efficient, and designed for future security needs.

MD5

The Message Digest 5 algorithm produces hashes that are **128 bits in length**, expressed as **32 hexadecimal characters**. Introduced in 1991.

SHA-1

Secure Hashing Algorithm-1 produces hashes that are **160 bits in length**, expressed as **40 hexadecimal characters**.

SHA-2

Secure Hashing Algorithm-256 produces hashes that are **256 bits in length**, expressed as **64 hexadecimal characters**.

Tools for calculation of Hash Function

HashMyFiles
https://www.nirsoft.net/utils/hash_my_files.html

Hash Calc
https://hashcalc.en.softonic.com/download

Gizmo Central
https://gizmo-central.en.softonic.com/download

https://md5file.com/calculator

Certificate u/s 63 (4) (c) of Bhartiya Sakshya Adhiniyam, 2023 regarding Admissibility of electronic and digital record

PART A

(To be filled by the Party)

I, _____ (Name), Son/daughter/spouse of _____ residing/employed at _____ do hereby solemnly affirm and sincerely state and submit as follows:—

I have produced electronic record/output of the digital record taken from the following device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____
Serial Number: _____
IMEI/UIN/UID/MAC/Cloud ID_____ (as applicable)
and any other relevant information, if any, about the device/digital record____(specify).

The digital device or the digital record source was under the lawful control for regularly creating, storing or processing information for the purposes of carrying out regular activities and during this period, the computer or the communication device was working properly and the relevant information was regularly fed into the computer during the ordinary course of business. If the computer/digital device at any point of time was not working properly or out of operation, then it has not affected the electronic/digital record or its accuracy. The digital device or the source of the digital record is:—

Owned ☐ Maintained ☐ Managed ☐ Operated ☐

by me (select as applicable).

I state that the HASH value/s of the electronic/digital record/s is _____, obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other_____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____hours (In 24 hours format)

Place: _____

Part-A

Certificate to be furnished by the Party

PART B

(To be filled by the Expert)

I, _____ (Name), Son/daughter/spouse of _____ residing/employed at _____ do hereby solemnly affirm and sincerely state and submit as follows:—

The produced electronic record/output of the digital record are obtained from the following device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____
Serial Number: _____
IMEI/UIN/UID/MAC/Cloud ID_____ (as applicable)
and any other relevant information, if any, about the device/digital record_____(specify).

I state that the HASH value/s of the electronic/digital record/s is _____, obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other_____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name, designation and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____hours (In 24 hours format)

Place: _____

Part-B

Certificate to be furnished by the Expert

Judgments

Video/Audio Tape Recordings:

Ziyauddin Burhanuddin Bukhari v Brijmohan Ramdass Mehra and Others [AIR 1975 SC 1788 (1)]

- The Hon'ble Supreme Court observed that **tape-recorded speeches are 'document', as defined by Section 3 of the Evidence Act**, which stands on having no different footing than photographs, and they are admissible in evidence on satisfying certain conditions.

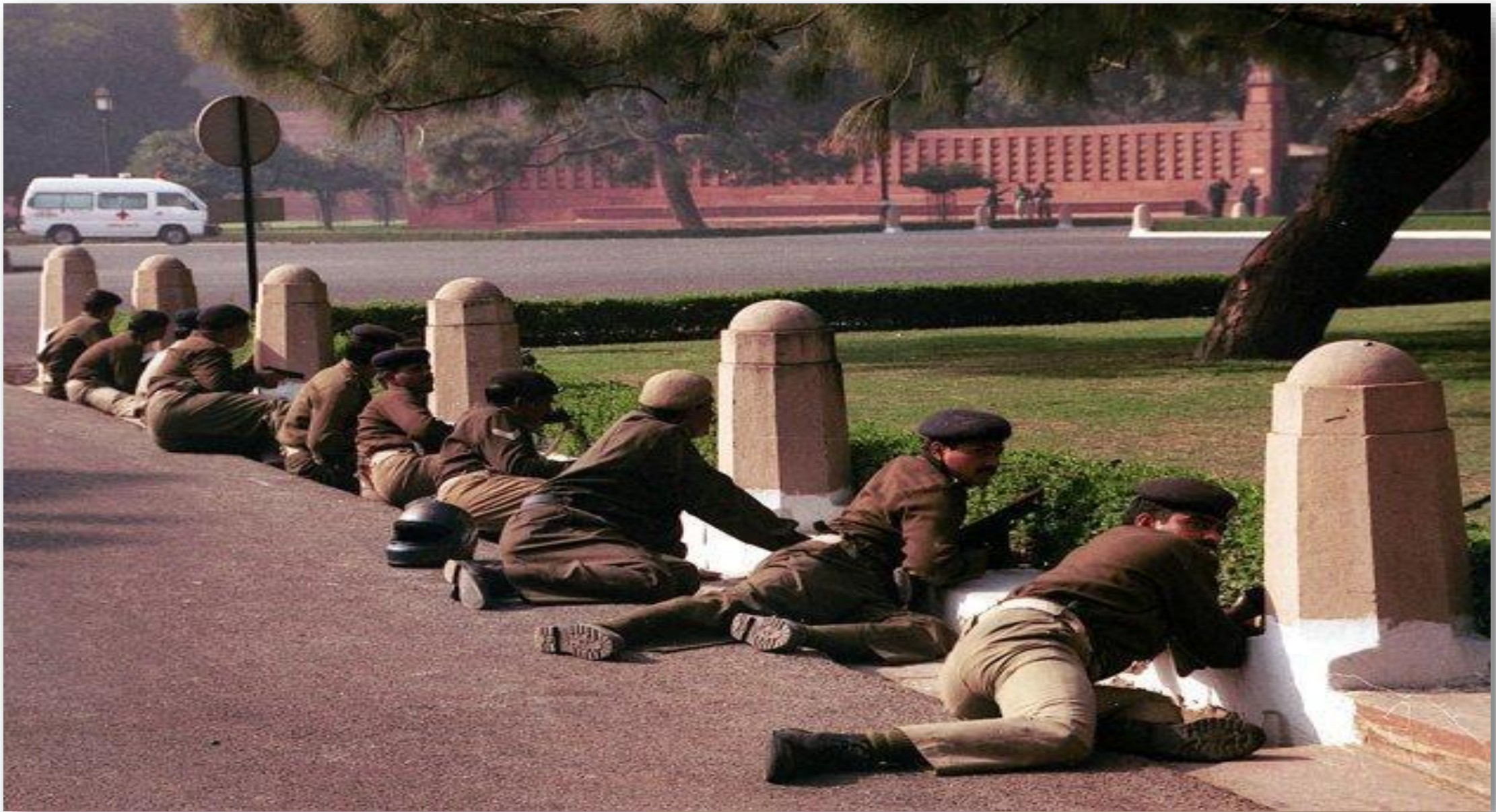
State (N.C.T. Of Delhi) vs Navjot Sandhu@ Afsan Guru

Appeal (crl.) 373-375 of 2004

BENCH: P. VENKATARAMA REDDI & P.P. NAOLEKAR

Supreme Court of India

Judgment dated 04.08.2005



State (NCT of Delhi) V. Navjot Sandhu alias Afzal Guru (2005) 11 SCC 600:

Even if the certificate containing the details mentioned in Section 65B of IEA is not provided, *secondary evidence can be given if it complies with the provisions under section 63 and 65 of the Act.*

Jagjit Singh Vs. State of Haryana [(2006) 11 SCC 1)]

This judgment is the era of beginning to recognize and appreciate the importance of digital evidence in legal proceedings.

Jagjit Singh Vs. State of Haryana [(2006) 11 SCC 1)]

- The speaker of the Legislative Assembly of the State of Haryana disqualified a Member for defection.
- While hearing the matter, the Supreme Court considered the digital evidence in the form of interview transcripts from the Zee News television channel, the Aaj Tak television channel and the Haryana News of Punjab Today television channel.
- The court determined that the *electronic evidence placed on record was admissible* and upheld the reliance placed by the Speaker on the recorded interview while reaching the conclusion that the *voices recorded on the CD were those of the persons taking action*. The Supreme Court found no infirmity in the Speaker's reliance on the digital evidence and the conclusions reached by him.

Dharambir

vs

Central Bureau Of Investigation

Crl. M. C. 1775/2006

148 (2008) DLT 289

By, THE HONOURABLE

DR. JUSTICE S. MURALIDHAR

Delhi High Court

Judgment dated 11th March, 2008

A hard disk of a computer is considered as documentary evidence:

Dharambir Vs. CBI [148 (2008) DLT 289]

A blank hard disc is an electronic device which is used for storing information and has once been used in any manner, for any purpose will contain some information and will, therefore, be an electronic record.

Anvar P.V vs P.K.Basheer & Ors

CIVIL APPEAL NO. 4226 OF 2012

Bench: Chief Justice, Kurian Joseph, Rohinton Fali Nariman

Supreme Court of India

Judgment dated 18 September, 2014

Anvar P.V v. P.K Basheer (2014)10 SCC473:

- Overrules State (NCT of Delhi)V. Navjot Sandhu (2005) 11 SCC 600
- Electronic record by way of *secondary evidence shall not be admitted in evidence unless the requirements under Section 65B of IEA are satisfied*. Since 65A and 65B of IEA are special provisions they will be given precedence over general laws in Sections 63 and 65 of IEA

(Generalia specialibus non derogant)

- Notwithstanding Sections 59, 65A and 65B of the Indian Evidence Act, an electronic record used as primary evidence under Section 62 is admissible in evidence, without complying Section 65B of the Evidence Act. (Para 22)
- Makes all of the conditions under Section 65B (4) imperative.

Tomaso Bruno & Anr. Vs. State of UP [(2015) 7 SCC 178]

- A three Judge Bench of the Apex Court by Judgment dated 20-1-2015, dealt with the admissibility of evidence in a criminal case. At paragraph No. 25 of the judgment, held that "secondary evidence of the contents of a document can also be led under Section 65 of the Evidence Act". The judgment led *CCTV footage* admissible in the case.

Kundan Singh v. State, 2015 SCC Delhi HC

- Section 65B certificate was submitted by the nodal officer of the concerned telecom agency at the time of his *re-examination* only.
- The court held that "a certificate under sub-section (4) to section 65B *must be issued simultaneously* with the production of the computer output or it can be issued and tendered when the computer output itself is tendered to be admitted as evidence in the court or, as in the present case, by the official when the accused was recalled to give evidence".

Paras Jain v. State of Rajasthan, 2015

- Rajasthan HC held that "the goal of a criminal trial is to discover the truth and to achieve that goal, the best possible evidence is to be brought on record.
- *Thus, in all the cases where the police have not filed the certificate under section 65B, the prosecution agency can file the certificate by way of supplementary charge sheet under section 173(8) of Cr PC.*

Shamsher Singh Verma vs State of Haryana

S.L.P. (Crl.) No. 9151 of 2015

Bench: Chief Justice of India Hon'ble Justice Sri Dipak Mishra & Hon'ble Justice Prafulla C. Pant

Supreme Court of India

Judgment dated 24.11.2015

- The 2-judge bench of the Hon'ble SC ruled that **"Compact Disc (CD) is also a document.**
- It is not necessary for the court to obtain admission or denial on a document under sub-section (1) to Section 294 of CrPC personally from the accused or complainant or the witness.
- It would be considered as erring so as to reject the application to play the compact disc in question to enable the public prosecutor to admit or deny, and to get it sent to the Forensic Science."

Abdul Rahaman Kunji V. State of West Bengal [2016 CLRJ 1159]

- High Court of Calcutta while deciding *admissibility of email* held that an email downloaded and printed from email account of the person can be proved by sec. 65B r/w Sec 88A of IEA.
- Testimony of witness to carry out such procedure to download and print the same is sufficient to prove communication.

Vikram Singh V. State of Punjab (2017) 8 SCC 518:

- *Tape recorded conversation* in this case was held to be primary evidence and not secondary evidence which required certificate under 65B of IEA.
- Reference to Anvar case: If an electronic evidence is used as primary evidence, the same is admissible in evidence, without compliance with the conditions in Section 65 B.

Sonu Vs State of Haryana (2017) 8 SCC 570

- ✓ A CDR without any certification under Section 65B is not inherently inadmissible.
- ✓ Such certification pertains to the mode and method of proof and objection thereto must be raised at the earliest stage. In the event of failure, objection cannot be raised at an appellate stage.
- ✓ Comments on necessity of prospective overruling and leaves the question of retrospective application of Anvar open for an appropriate bench as Anvar was a larger bench.

SHAFHI MOHAMMAD Vs THE STATE OF HIMACHAL PRADESH

SPECIAL LEAVE PETITION (CRL.)No.2302 of 2017 with SLP(Crl) No. 9431/2011 & SLP(Crl) No(S). 9631-9634/2012

Bench: ADARSH KUMAR GOEL & UDAY UMESH LALIT

SUPREME COURT OF INDIA

Judgment dated January 30, 2018

Shafhi Mohammad V. State of U.P (2018) 1 SCC (Cri) 860

- Requirement of certificate being procedural can be relaxed by the court wherever the interest of justice so justifies. (Example; Bills generated in shops, electronic tickets etc.)
- Procedural requirement under Section 65B(4) of Evidence Act of furnishing certificate is to be applied only when electronic evidence is produced by a person who is in a position to produce such certificate being in control of the said device.
- When the party is not in possession of such a device, applicability of Section 63 and 65 of the Evidence Act cannot be held to be excluded.
- Refers P.V. Anvar to larger bench.

State of Karnataka Lokayukta Police Station, Bengaluru V. R. Hiremath,
[Criminal Appeal No. 819 of 219; 2019 SCC OnLine SC734]

- ✓ Certificate under 65(B) can be supplied subsequent to filing of charge sheet. Production of such a certificate is required when the electronic record is sought to be produced in evidence at the trial.

- *The High Court erred in coming to the conclusion that the failure to produce a certificate under Section 65-B(4) of the Evidence Act at the stage when the charge-sheet was filed was fatal to the prosecution.*
- *The need for production of such a certificate would arise when the electronic record is sought to be produced in evidence at the trial. It is at that stage that the necessity of the production of the certificate would arise.*

Om Prakash Verma V. State of West Bengal and Ors. [2017(4) CALCRILR 61; 2018 CRLJ 640]

Preservation of Evidence

- ✓ When electronic devices like mobile phone, laptop, tablet, etc. are seized as stolen property and are required to be produced and identified during trial, interim custody of such devices pending investigation, enquiry or trial shall not be granted till the IMEI number or other unique identification number, and its brand/product number and manufacturing details is ascertained and noted in the case records for identification of such device during trial.

Subhendu Nath V. State of West Bengal [MANU/WB/0500/2019; 2019(2) RCR (Criminal) 112]

Preservation of Evidence

- A breach in the chain of custody or improper preservation of such evidence renders electronic evidence vitiated unreliable in judicial proceedings.
- Necessary certification under Section 65B of IT Act is also a prerequisite for admissibility of such evidence.
- Even in case of certification, reliability of electronic evidence depends on proper collection , preservation and production in court and any lacuna in that regard would render such evidence vulnerable with regard to its probative value.

IN THE SUPREME COURT OF INDIA

CIVIL APPELLATE JURISDICTION

CIVIL APPEAL NOS. 20825-20826 OF 2017

ARJUN PANDITRAO KHOTKAR ...Appellant

Versus

KAILASH KUSHANRAO GORANTYAL AND ORS. ...Respondents

WITH

CIVIL APPEAL NO.2407 OF 2018

CIVIL APPEAL NO.3696 OF 2018

Judgment dated 14.07.2020

ARJUN PANDITRAO KHOTKAR Vs. KAILASH KUSHANRAO GORANTYAL AND ORS. [2020 SCC OnLine SC 571]

A Three-Judge Bench of the Hon'ble apex court by Judgment dated July 14, 2020, upheld the law laid in Anwar PV's case. Paragraph No.72 contains the relevant observations. They are extracted hereunder:

*(a) Anvar P.V. (supra), as clarified by us hereinabove, is the law declared by this Court on Section 65B of the Evidence Act. The judgment in **Tomaso Bruno** (supra), being per incuriam, does not lay down the law correctly. Also, the judgment in SLP (Crl.) No. 9431 of 2011 reported as **Shafhi Mohammad** (supra) and the judgment dated 03.04.2018 reported as (2018) 5 SCC 311, do not lay down the law correctly and are therefore **overruled**.*

(b) The clarification referred to above is that the required certificate under Section 65B(4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him.

In cases where the "computer" happens to be a part of a "computer system" or "computer network" and it becomes impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4).

The last sentence in Anvar P.V. (supra) which reads as "...if an electronic record as such is used as primary evidence under Section 62 of the Evidence Act..." is thus clarified; it is to be read without the words "under Section 62 of the Evidence Act,..." With this clarification, the law stated in paragraph 24 of Anvar P.V. (supra) does not need to be revisited."

Some other highlighted Judgments

Don’t register FIR u/s 66A of Information Technology Act

- A Division Bench of Supreme Court consisting of Justices J. Chelameswar and R.F. Nariman decided on 24th March, 2015 in Shreya Singhal v. Union of India to struck down section 66A of Information Technology Act, 2000 (21 of 2000) as **unconstitutional**, as it is violative of Article 19(1)(a) related to freedom of speech and expressions.
- Now comments on social networking sites will not be offensive unless they come under the provisions of the Indian Penal Code.

K. Ramajayam v. Inspector of Police

Referred Trial 1/2015, Cr A 110/2015

In the High Court of Judicature at Madras

Justice R. Sudhakar and Justice P. N. Prakash

January 27, 2016

- The bench was of the opinion that electronic evidence may not be clearly specified in Section 2(t) of the IT Act, 2000, but in certain cases, the entire servers cannot be brought into the courtrooms.
- In the present case, the accused was clearly caught on camera during the commission of his offence and therefore, the **CCTV footage must be considered as electronic evidence.**

CRIMINAL APPEAL NOS. 2161-2162 OF 2024

(SPECIAL LEAVE PETITION (CRL.) NOS. 3665-3666 OF 2024)

JUST RIGHTS FOR CHILDREN ALLIANCE & ANR.
...APPELLANT(S)
VERSUS
S. HARISH & ORS. ...RESPONDENT(S)

Supreme Court of India

Judgment Dated: 23rd September, 2024

Hon'ble CJI Dr. Dhananjaya Y. Chandrachud and Hon'ble Justice J.B. Pardiwala

(i) The Parliament should seriously consider to bring about an amendment to the POCSO for the purpose of substituting the term “child pornography” that with **“child sexual exploitative and abuse material” (CSEAM)** with a view to reflect more accurately on the reality of such offences. The Union of India, in the meantime may consider to bring about the suggested amendment to the POCSO by way of an ordinance.

(ii)We put the courts to notice that the term “child pornography” shall not be used in any judicial order or judgment, and instead the term “child sexual exploitative and abuse material” (CSEAM) should be endorsed.

IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO 494 OF 2012

JUSTICE K S PUTTASWAMY (RETD.), AND ANR.
..Petitioners
VERSUS
UNION OF INDIA AND ORS. ..Respondents

Judgment dated: 24th August, 2017

- A nine-judge Constitution Bench headed by Chief Justice J.S. Khehar on 24th August, 2017 gave a landmark decision on Right to Privacy.
- Supreme Court ruled that Right to Privacy is **"intrinsic to life and personal liberty"** and **is inherently protected under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution**.
- Reading out the common conclusion arrived at by the nine-Judge Bench, the Chief Justice said the Court had overruled its own eight Judge Bench and six-Judge Bench judgments of M.P. Sharma and Kharak Singh cases delivered in 1954 and 1961 respectively that privacy is not protected under the Constitution.
- To overcome these two precedents, a five-judge Bench led by Chief Justice J.S. Khehar had referred the question whether privacy is a fundamental right or not to the numerically superior nine-Judge Bench.

JOIN LATEST JUDGMENTS FOR LAWYERS
WHATSAPP GROUP @ 7347447651

JOIN LATEST JUDGMENTS FOR LAWYERS
WHATSAPP GROUP TO UPDATE YOURSELF FOR:

LATEST LEGAL UPDATES,
JOB ALERTS,
INTERNSHIP NOTIFICATIONS,
NOTES,
PDF FILES,
LAW RELATED VIDEOS,
LEGAL DRAFTS,
JUDGMENTS OF SUPREME COURT
&
HIGH COURTS OF INDIA.

PLEASE CONTRIBUTE PERMANENT
MEMBERSHIP FEES (LIFETIME) OF RS 999/-
ONLY TO JOIN THE GROUP.

PAY THROUGH GOOGLE PAY/PHONEPE/ PAYTM
@ MOB. 7347447651.

CONTRIBUTE PERMANENT MEMBERSHIP FEES (LIFETIME) OF
Rs 999/- ONLY TO JOIN THE GROUP.
PAY THROUGH GOOGLE PAY/PHONEPE/ PAYTM @ MOB 7347447651

Thanks

yak, OPS
3PSPA
4033879