eAuthentication Frameworkin e-GP Issues in Security and Interoperability

electronic Vs Digital Signatures

K Srinivasa Raghavan
National Informatics Centre, India
raghavan@gov.in

3rd Oct 2017
TBILISI, Georgia

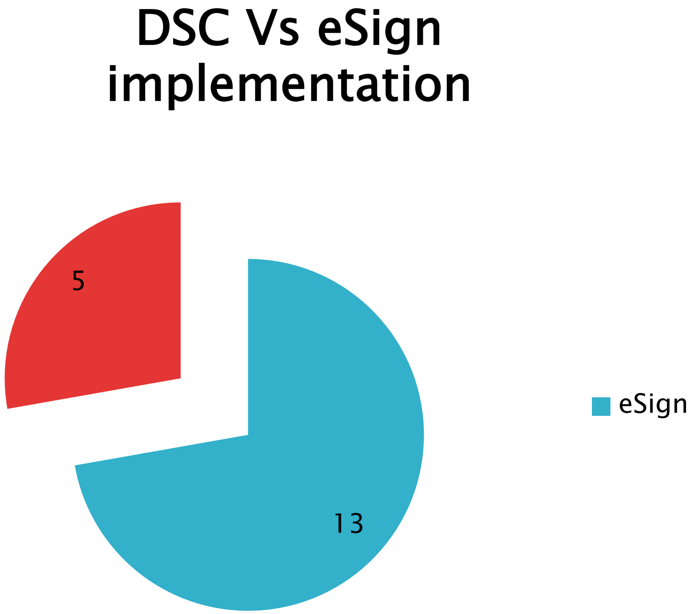
Agenda

- Need for eAuthentication
  - eSign
  - Encryption of Bids
- eAuthentication Framework Methodology
- Legal Aspects / Technology Aspects
- Emerging Technologies

eSign – Login Authentication

- UserName and Password Based login

Five countries in addition have implemented Digital Signature based login



With DSC	eSign based
Malaysia, Mongolia India, Kazakhstan & Vietnam	Bangladesh, Bhutan, Cook Islands Fiji, Georgia, Kyrgyz Republic, Nepal, Phillipines, Tajikistan, Thailand,Tuvalu, Uzbekistan, Vanuatu,

Methods of Bid Encryption

Following two methods of encryption are adopted

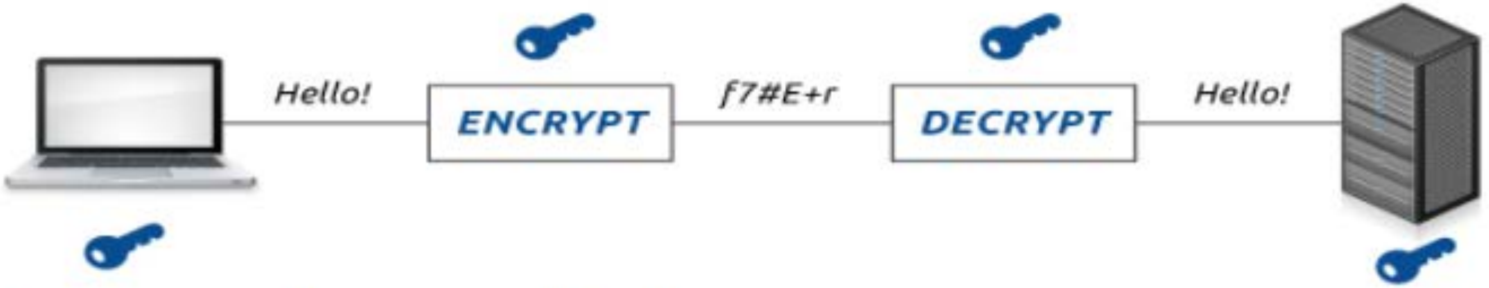
- Symmetric Encryption
- Asymmetric Encryption

Securing Bids – Symmetric Encryption

- Symmetric Encryption
  - Conceptually Simple- Hash Gets Generated
  - Easy to Implement
  - Meets basic Security Needs

Symmetric Key Encryption

Sample AES encryption



Source: http://tinyurl.com/k2m4bed

S.no.	Plain Text	Cipher Text	Key
1	Hello World	fgvVrcbUInFnkyXuZckNcQ==	Ram
2	Long long text abcd	jxqe2RkCoB/+pNEG+MmrMIUgbYTP5uP8KRryJz75+/s=	Ram

Two-way function

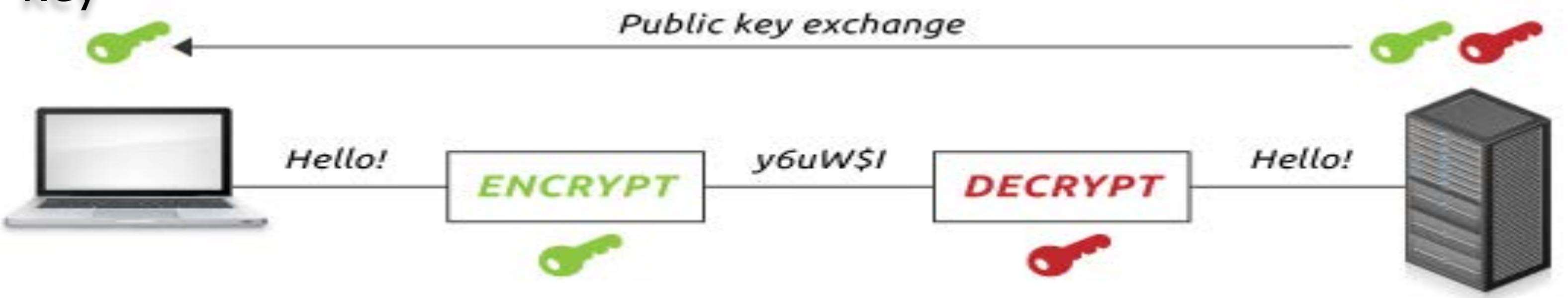
Key involved: Symmetric

Risk: If key is compromised, anyone can read the message (i.e. plain text)

Asymmetric Key Encryption

Encryption done by sender using public key of recipient

Recipient will decrypt using corresponding private key



Source: http://tinyurl.com/k2m4bed

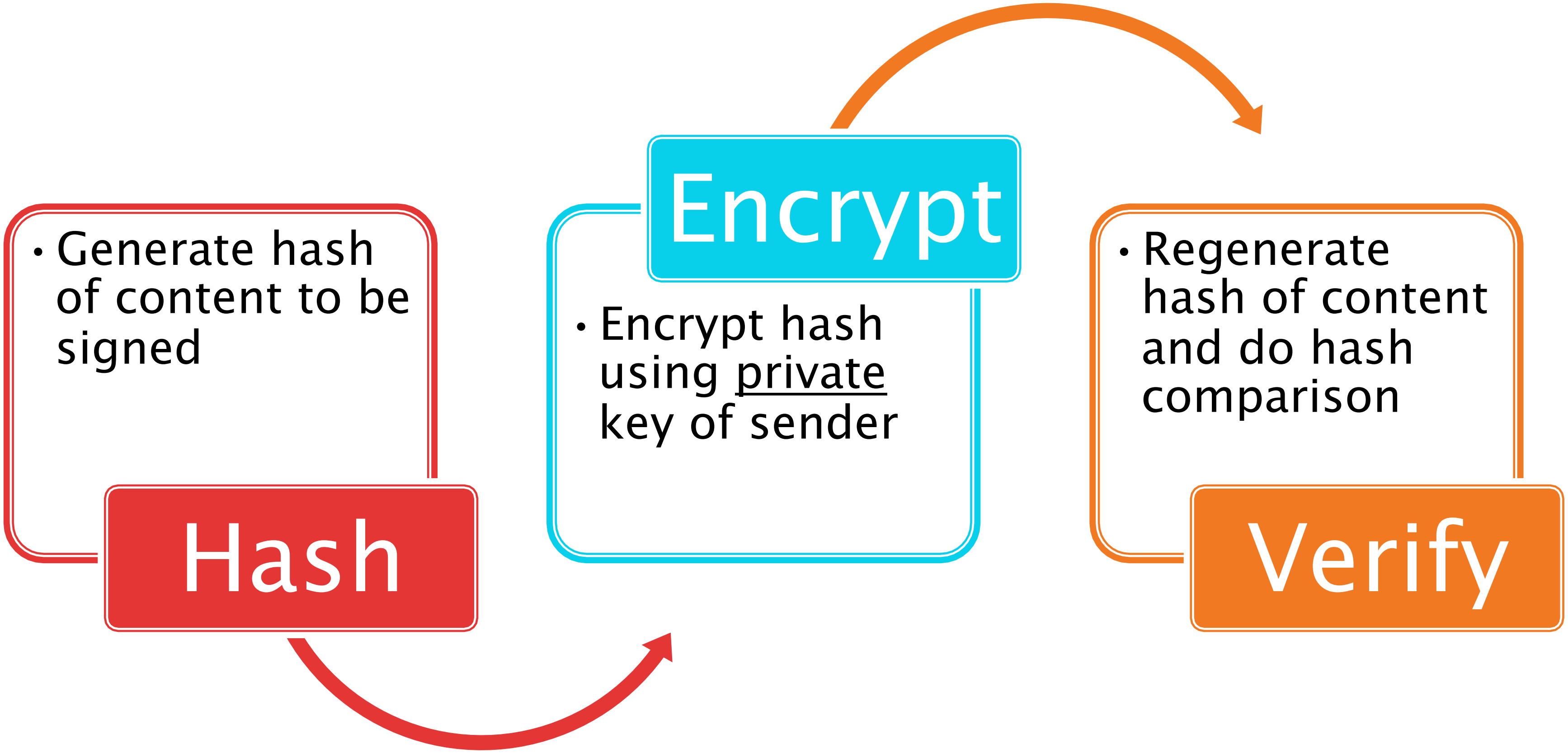
Two-way function

Private-public key pair is certified and attributed to a person in a DSC

Supplier encrypt its financial quote using public key of the Tender Inviting Authority (TIA)

The TIA will open the financial quote after tender opening using the corresponding private key. Only the TIA can open and no one else.

Digital Signature



Hash

- Generate hash of content to be signed

Encrypt

- Encrypt hash using private key of sender

Verify

- Regenerate hash of content and do hash comparison

Encrypted hash is digital signature

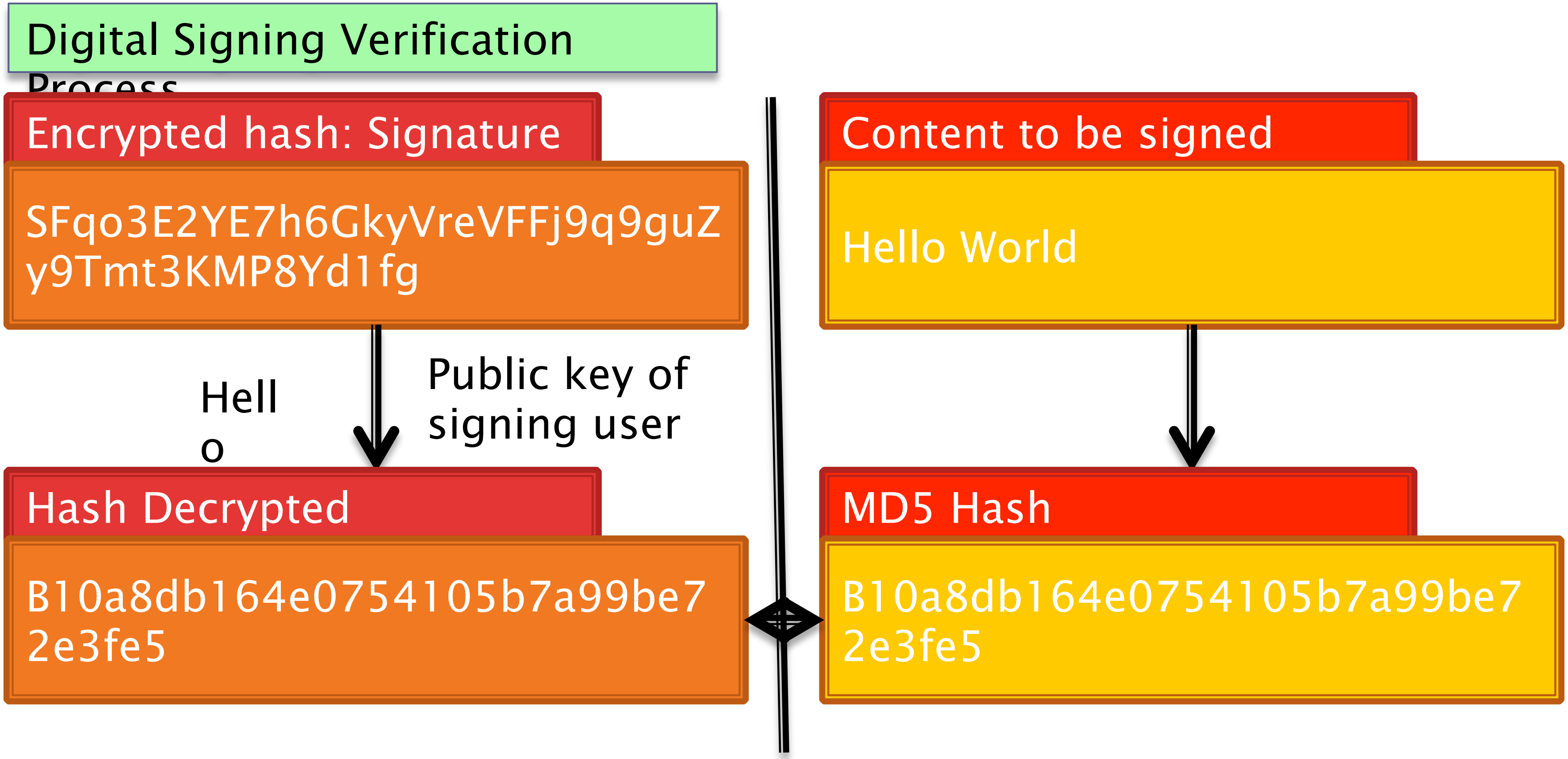
If hash does not match, sender can argue that the content has been tampered with

Digital Signature -- Sample

Digital Signing Process

Content	Hello World
MD5 Hash	B10a8db164e0754105b7a99be72e3fe5
Encrypt key	Symmetric: “Hello” Asymmetric key: Private key of signing user
Encrypted Hash (Signature)	SFqo3E2YE7h6GkyVreVFFj9q9guZy9Tmt3KMP8Yd1fg=

Digital Signature Verification Process



Digital Signing Verification Process

Encrypted hash: Signature

SFqo3E2YE7h6GkyVreVFFj9q9guZy9Tmt3KMP8Yd1fg

Hell
o

Public key of signing user

Hash Decrypted

B10a8db164e0754105b7a99be72e3fe5

Content to be signed

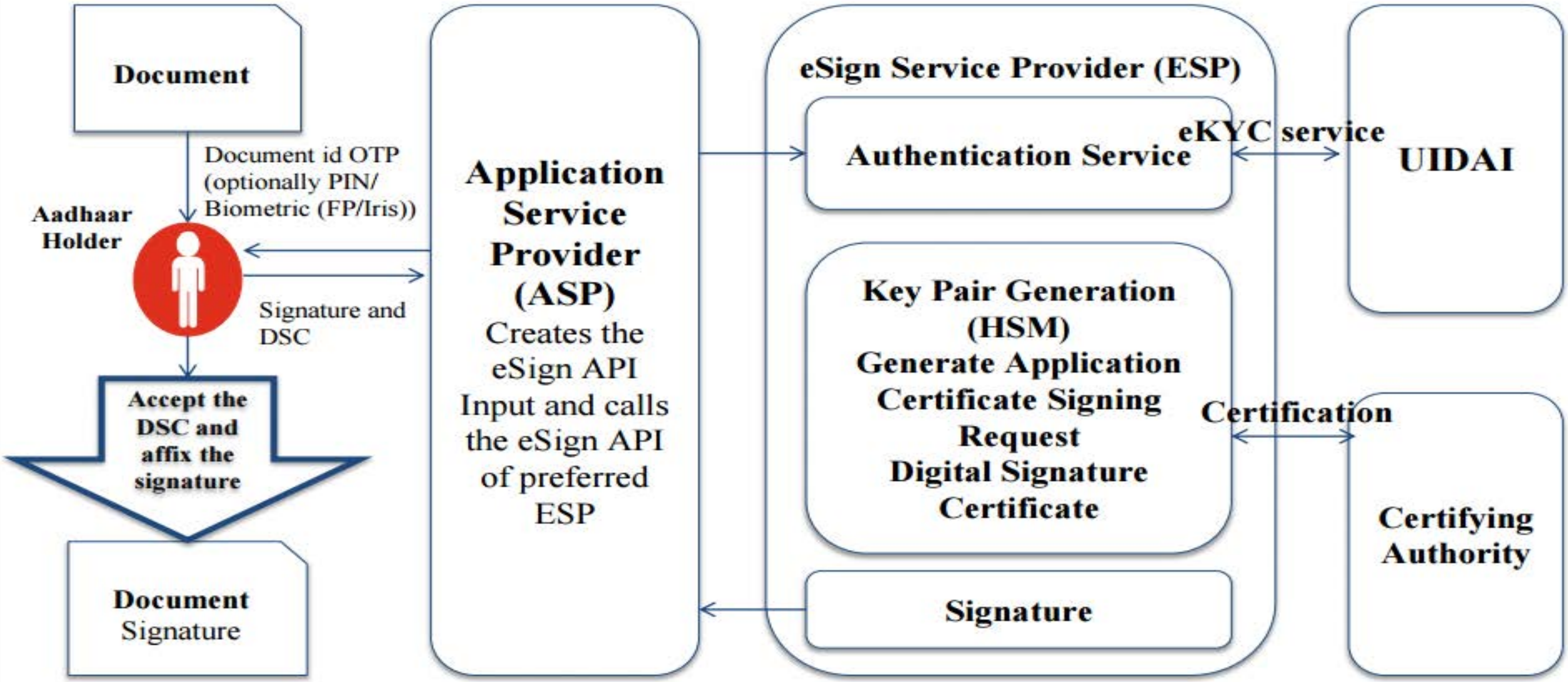
Hello World

MD5 Hash

B10a8db164e0754105b7a99be72e3fe5

When Hash matches, it is confirmed that the content is signed by the said person

e-Sign



HSM – Hardware Security Module
OTP – One Time Password
ESP – eSign Service Provider
ASP – Application Service Provider
eKYC – electronic Know Your Customer
DSC – Digital Signature Certificate
FP – Finger Print
UIDAI – Unique Identification Authority of India

Source: CCA

Content to be signed is passed in the API

Encrypted hash of the content is received back in signature

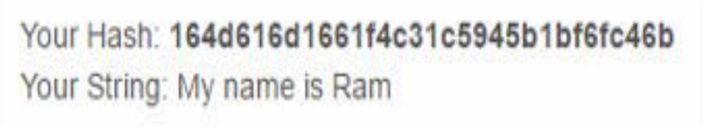
Both AADHAAR KYC and e-Sign happens real-time

New certificate generated every time

Should cost around 15-20 Rs per

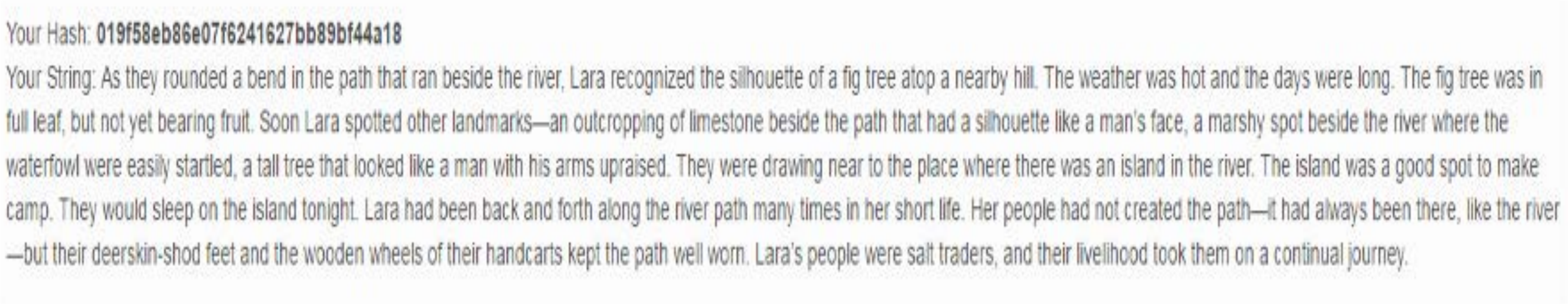
Hash Function

MD5 Hashing Algorithm



Your Hash: **164d616d1661f4c31c5945b1bf6fc46b**

Your String: My name is Ram



Your Hash: **019f58eb86e07f6241627bb89bf44a18**

Your String: As they rounded a bend in the path that ran beside the river, Lara recognized the silhouette of a fig tree atop a nearby hill. The weather was hot and the days were long. The fig tree was in full leaf, but not yet bearing fruit. Soon Lara spotted other landmarks—an outcropping of limestone beside the path that had a silhouette like a man's face, a marshy spot beside the river where the waterfowl were easily startled, a tall tree that looked like a man with his arms upraised. They were drawing near to the place where there was an island in the river. The island was a good spot to make camp. They would sleep on the island tonight. Lara had been back and forth along the river path many times in her short life. Her people had not created the path—it had always been there, like the river —but their deerskin-shod feet and the wooden wheels of their handcarts kept the path well worn. Lara's people were salt traders, and their livelihood took them on a continual journey.

Fixed length: 32 characters, 128 bits

One-way function

Securing Bids- Asymmetric Encryption

- Asymmetric Encryption

CA – Certifying Authority Needs to be set up

PKI – Public Key Infrastructure

  - Two Key Pairs (Public Key and Private Key)
  - Documents are encrypted using Public Key and decrypted using Private Keys.
  - Legal Framework should be modified to accept the PKI as equivalent as Physical Signatures

Securing Bids- Asymmetric Encryption

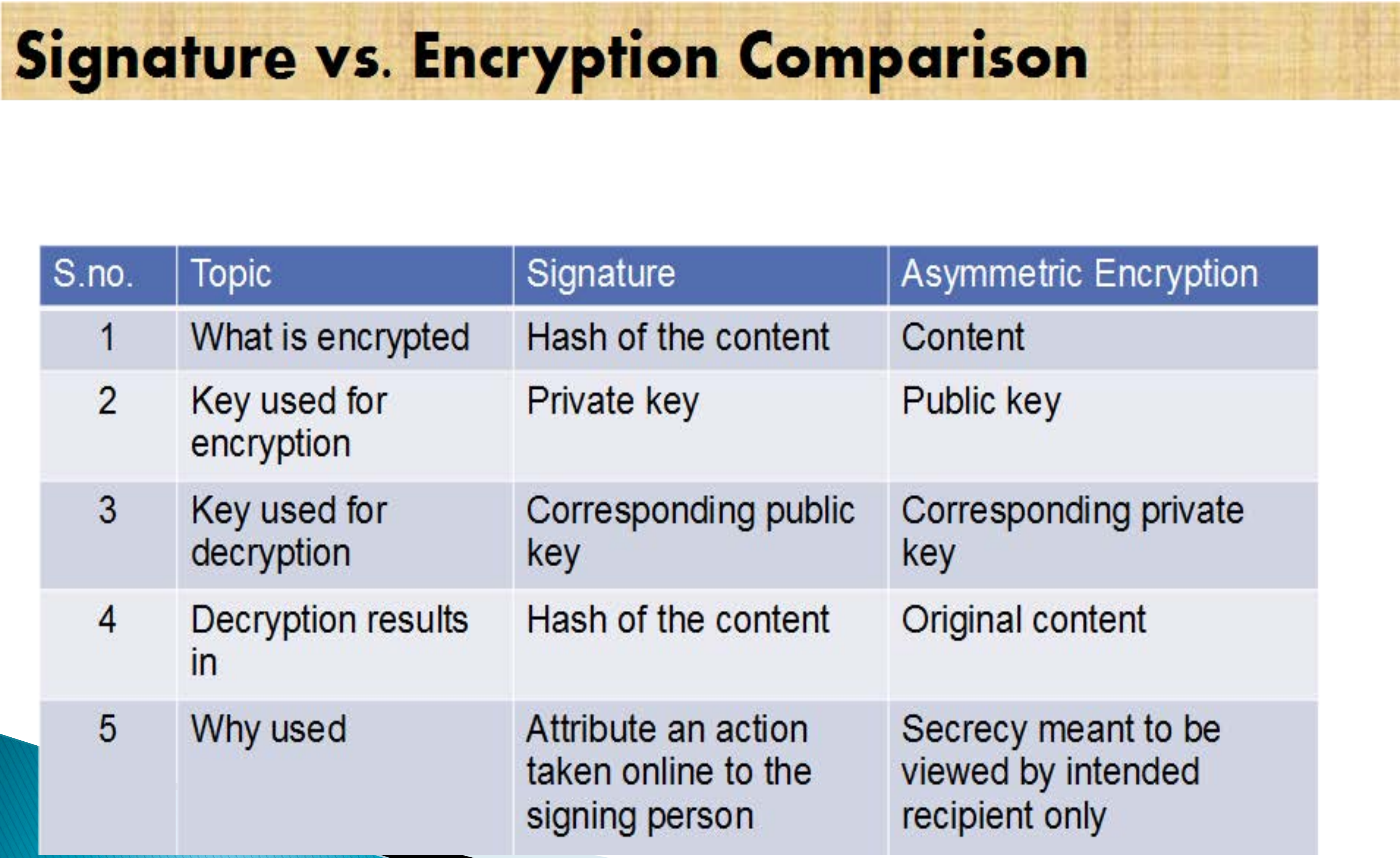
- Asymmetric Encryption

Technology Requirements

-Requires lots of Dependencies on Java, extra programming efforts

- Security is high at the cost of less convenient User Interfaces.
- Browser Issues to be resolved
- Support for Applets withdrawn

Signing Vs Encryption



Signature vs. Encryption Comparison

S.no.	Topic	Signature	Asymmetric Encryption
1	What is encrypted	Hash of the content	Content
2	Key used for encryption	Private key	Public key
3	Key used for decryption	Corresponding public key	Corresponding private key
4	Decryption results in	Hash of the content	Original content
5	Why used	Attribute an action taken online to the signing person	Secrecy meant to be viewed by intended recipient only

Emerging Technologies

- **Hardware Security Modules**:

  A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing. These **modules** traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server.

- **Block Chain Technology**

  A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. A network of so-called computing “nodes” make up the blockchain.

eprocurement

Public Key Infrastructure (’PKI’)

☑ System generates hash for each filename and signs the hash with bidder’s private key

☑ System generates hash for the content of each file and sign the hash with bidder’s private key

☑ System generates hash for encrypted document using the symmetric key to ensure the data integrity over the network layer

☑ System also generates hash for the encrypted symmetric key using bid openers public keys

Thank You

raghavan@gov.in