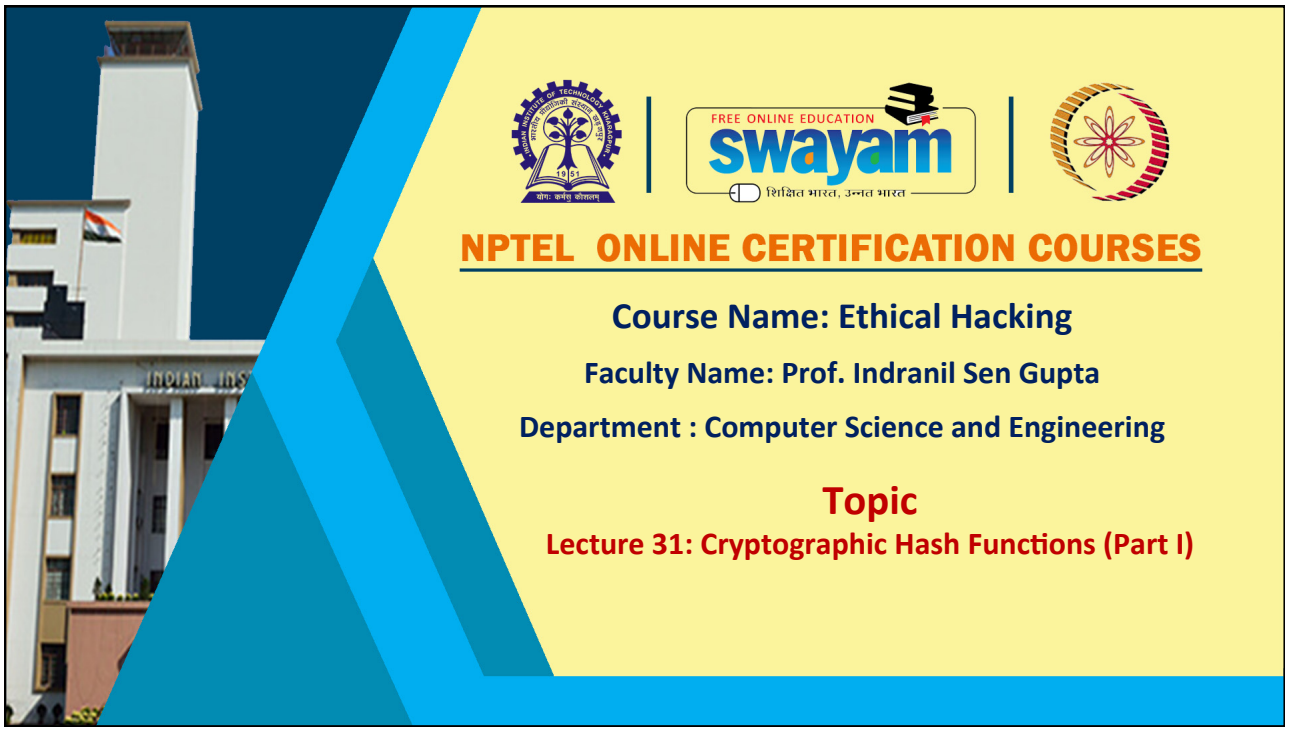


NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

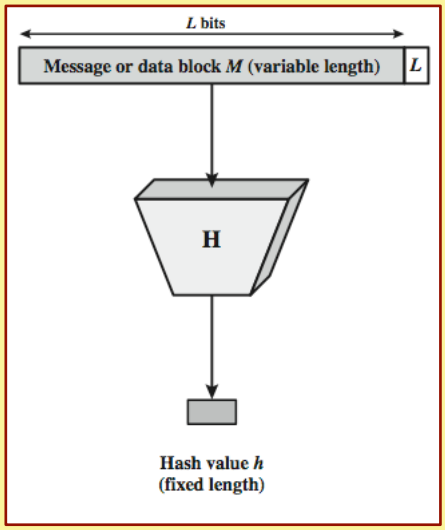
Lecture 31: Cryptographic Hash Functions (Part I)

CONCEPTS COVERED

- Desirable properties of hash functions
- Keyed and un-keyed hash functions

What are hash functions?

- They are computational functions that determine a hash digest *H* from a given message *M*.
  - The size of *M* is typically much larger than that of *H*.
- Also referred to as one-way functions.
  - Implement a many-to-one mapping.
  - Not possible to uniquely retrieve *M* from *H*.
- Cryptographic hash functions are hash functions with some desirable properties.


What is authentication?

- A process through which the identity of the sender can be confirmed.
  - Often makes use of cryptographic hash functions.
- Why required?
  - Many applications require one of the parties to confirm the identity of the other party.
  - Security applications heavily use authentication.
- We discuss authentication methods using cryptographic techniques.
  - Other methods like biometric authentication require physical presence of the sender.


5

Approaches to Message Authentication

a) Authentication using conventional encryption.
   - Only the sender and receiver should share a key.

b) Message authentication without message encryption.
   - An authentication tag is generated and appended to each message.

c) Message authentication code.

   Calculate the MAC as a function of the message and the key:

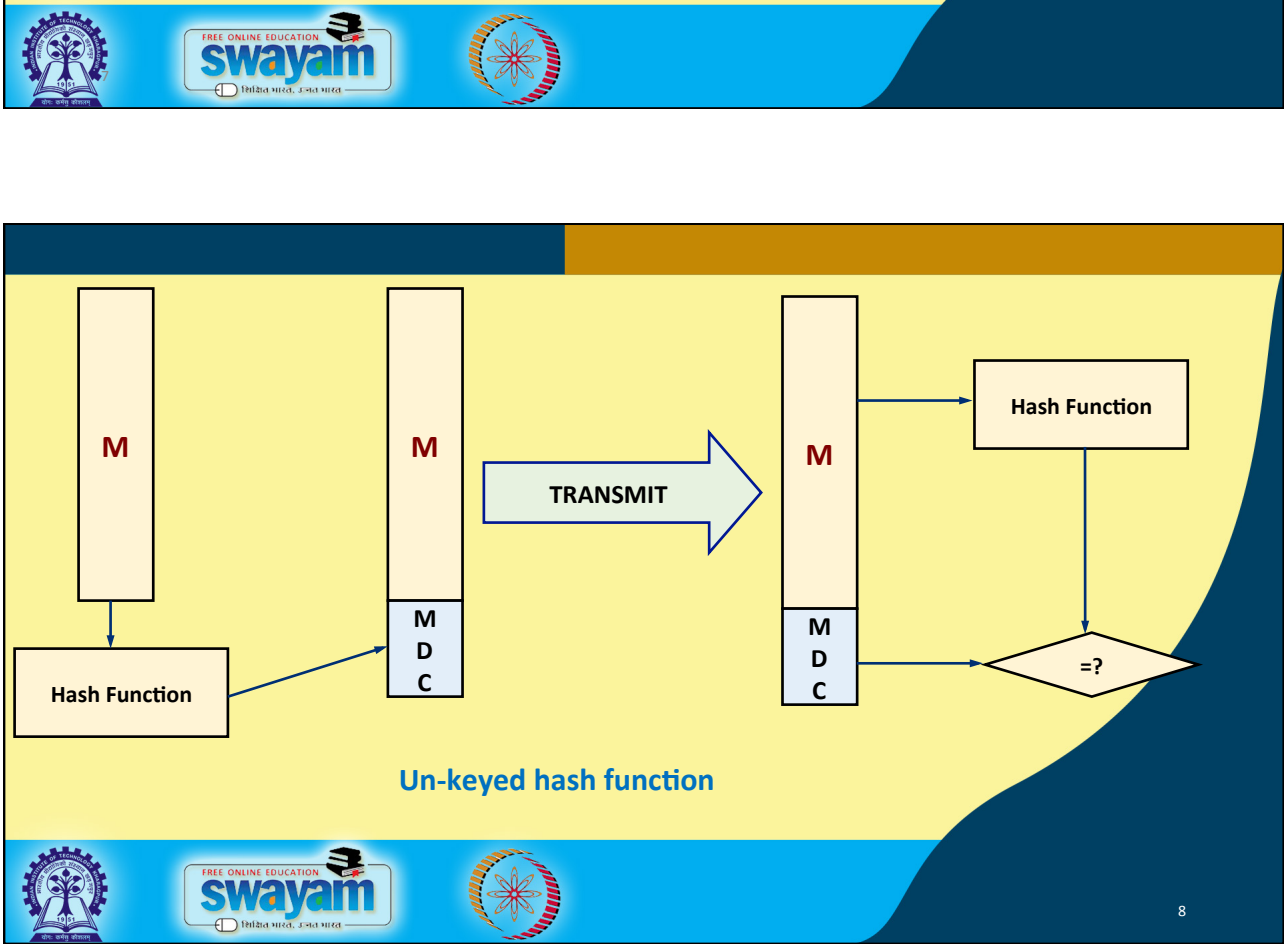
   MAC = F (K, M)


6

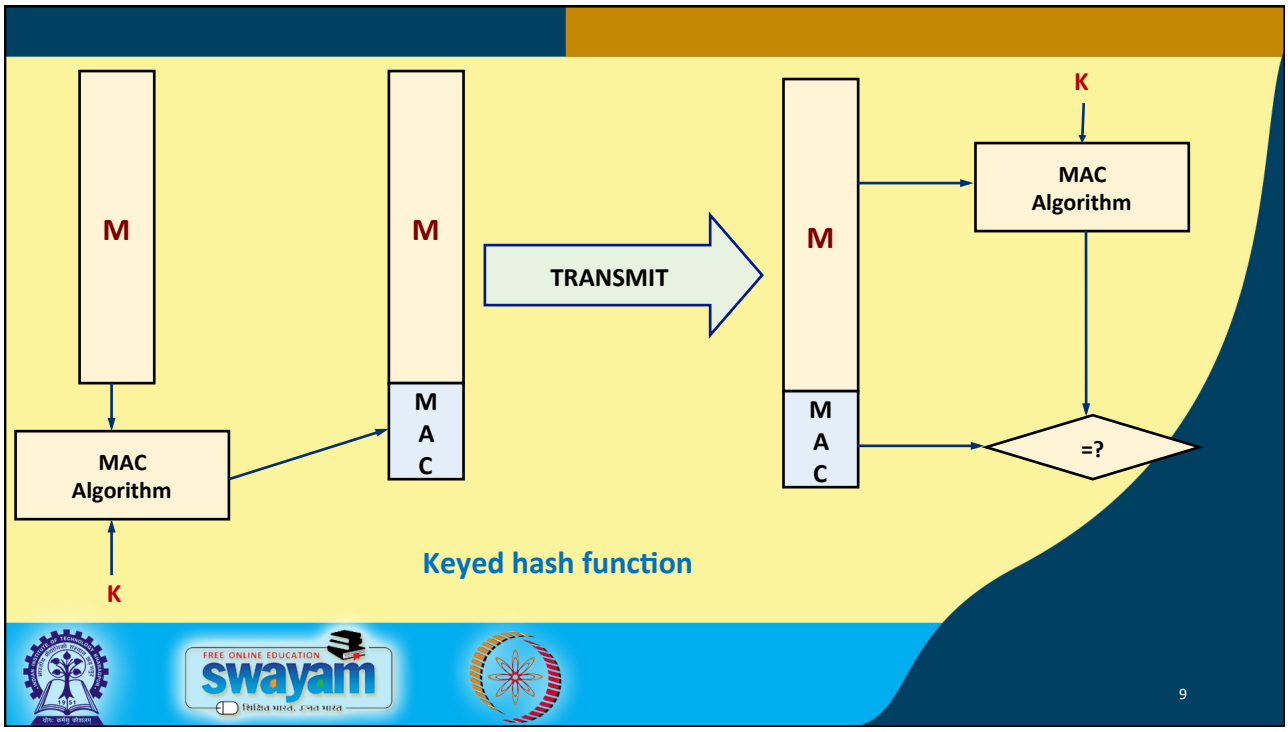
Hash Functions: Classification

a) Unkeyed hash function or *modification detection code* (MDC):
   - Used to preserve integrity of message.

b) Keyed hash function or *message authentication code* (MAC):
   - Used to authenticate the source of a message in addition to preserving integrity of the message.



Un-keyed hash function



Cryptographic Hash Functions: Desirable Properties

- **Collision**:
  - A hash function *H* maps an infinite set to a finite set.
  - So there must exist messages *x* and *x'* such that *H(x) = H(x')*.
  - Such a pair *(x, x')* of messages is called a ***collision*** for *H*.
- **First preimage resistance:**
  - Except for few hash values *y*, it should be difficult to find a message *x* such that *H(x) = y*.

- **Second preimage resistance:**
  - Given a message *x*, it should be difficult to find another message *x'* with the property that *H(x) = H(x')*.
- **Collision resistance:**
  - It should be difficult to find two messages *x* and *x'* with *H(x) = H(x')*.


To summarize ,,,

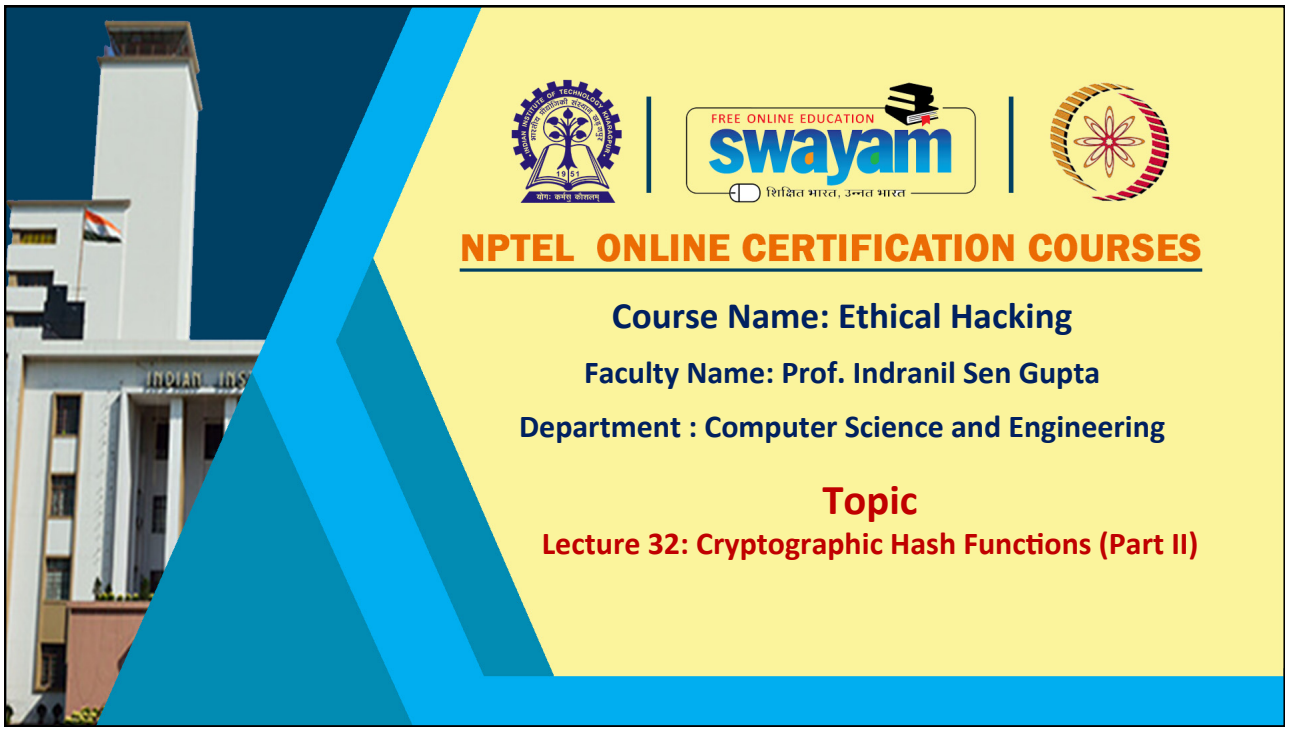
- Desirable properties of a cryptographic hash function *H*:
  a) The function *H* can be applied to a block of data at any size.
  b) The function *H* produces a fixed length output.
  c) The value *H(x)* is easy to compute for any given *x*.
  d) For any given block *x*, it is computationally infeasible to find *x* such that *H(x) = h*.
  e) For any given block *x*, it is computationally infeasible to find some block *y*, with *H(y) = H(x)*.
  f) It is computationally infeasible to find any pair *(x, y)* such that *H(x) = H(y)*, $x \neq y$.


Hash Functions: Examples

- Custom-designed hash functions work based on the general principle described earlier.
- Various families of hash functions:
  a) The MD family: MD2, MD4 and MD5 (128-bit hash).
  b) The SHA family: SHA-1 (160-bit), SHA-256 (256-bit), SHA-384 (384-bit) and SHA-512 (512-bit).
  c) RIPEMD-128 (128-bit), RIPEMD-160 (160-bit).

13

14



NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 32: Cryptographic Hash Functions (Part II)

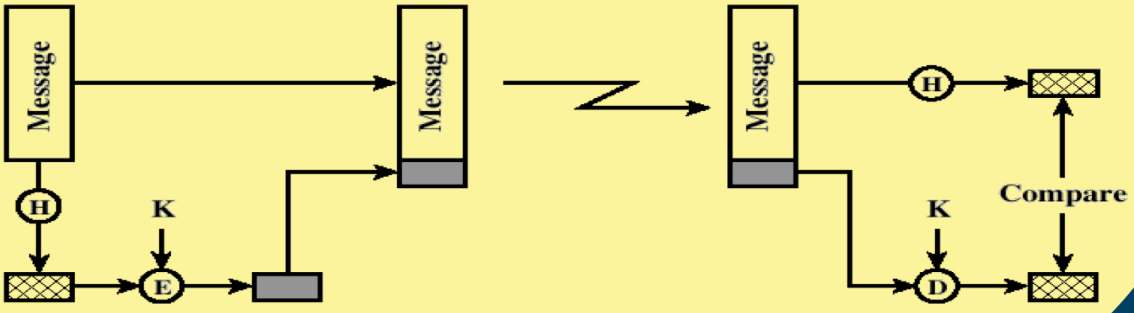
CONCEPTS COVERED

- Types of one-way hash functions
- SHA-512
- HMAC

One-way Hash Functions

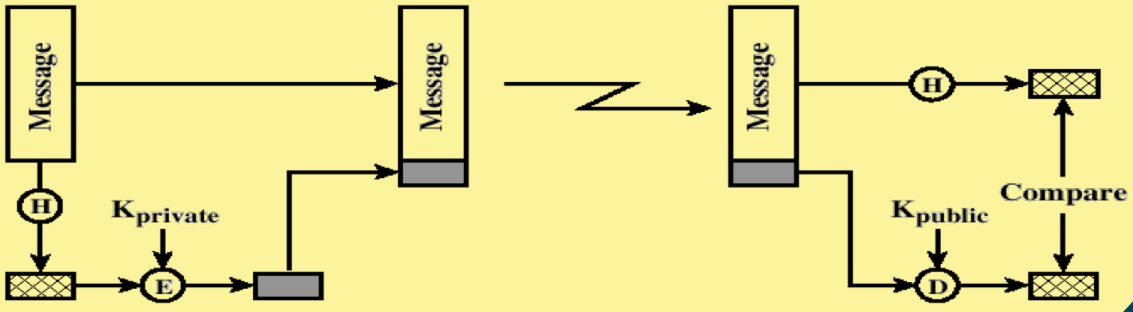
- We discuss various ways to implement one-way hash functions.
  - Using cryptographic techniques in addition to a hash function.
- Point to note:
  - Encryption and decryption are slower than hash computation.
  - Public-key encryption is slower than symmetric-key encryption.


One-way Hash Function



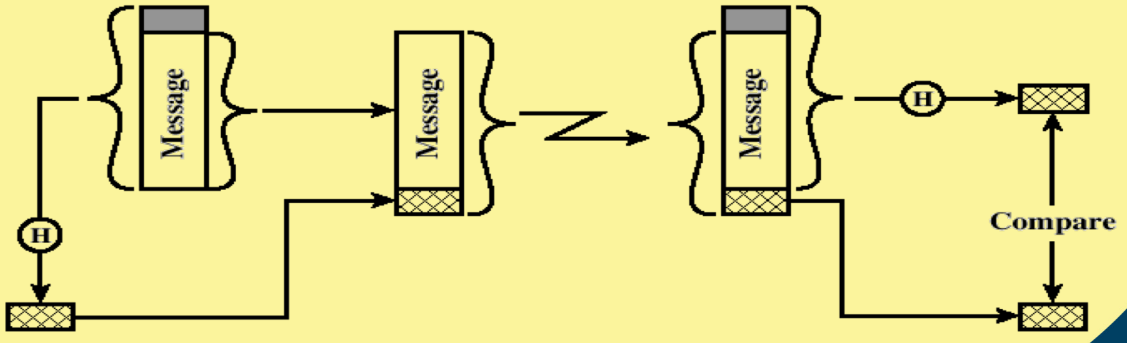
Using symmetric-key encryption


One-way Hash Function



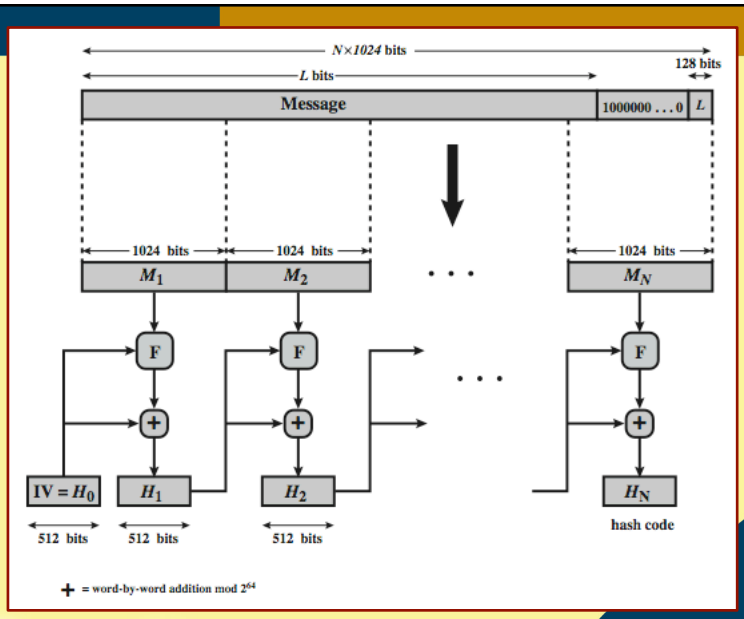
Using public-key encryption

One-way HASH function



Using a secret value (avoid encryption)

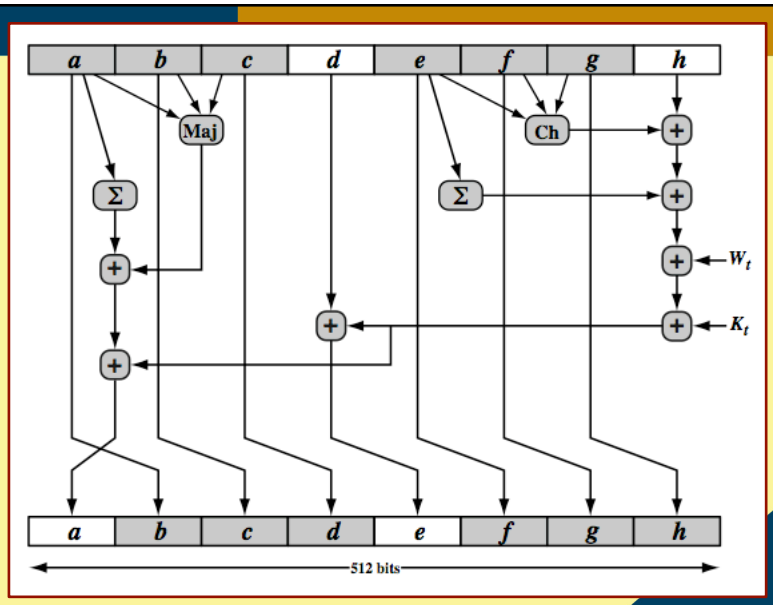
A case study: the SHA-512 algorithm



SHA-512 Compression Function

- Basic building block of the algorithm.
- Processes the message in 1024-bit blocks.
- Consists of 80 rounds (for each 1024-bit block)
  - Updating a 512-bit buffer.
  - Using a 64-bit value Wt derived from the current message block.
  - Also using a round constant based on the cube root of first 80 prime numbers.

SHA-512 Round Function



SHA Versions

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Digest length	160 bits	224 bits	256 bits	384 bits	512 bits
Basic unit of processing	512 bits	512 bits	512 bits	1024 bits	1024 bits
Number of steps	80	64	64	80	80
Maximum message size	2^{64}-1 bits	2^{64}-1 bits	2^{64}-1 bits	2^{128}-1 bits	2^{128}-1 bits

A case study: HMAC

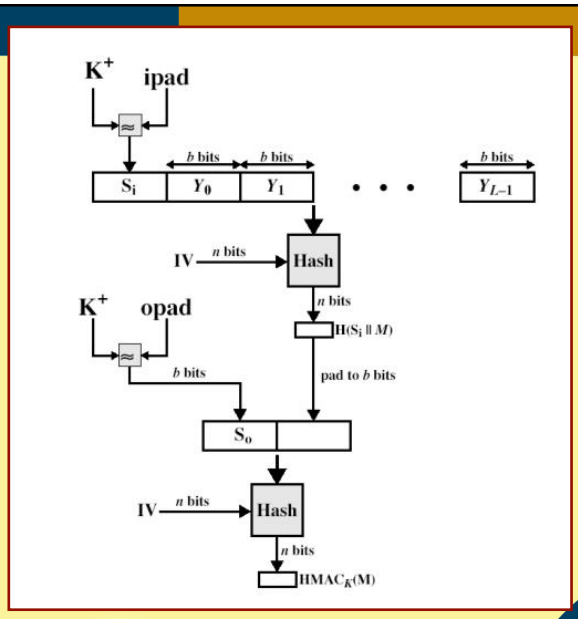
- Use a MAC derived from a cryptographic hash code, such as SHA-1.
- Motivations:
  - Cryptographic hash functions executes faster in software than encryption algorithms such as DES/AES.
  - Library code for cryptographic hash functions is widely available.


- HMAC (a keyed hash function)
- Notations:

  M = the message to be hashed
  H = an unkeyed hash function
  K = key for HMAC
  P, Q = short padding blocks (not secret).

  HMAC (M) = H (K || P || H (K || Q || M)).
- HMAC involves two calls of *H*.
- HMAC is efficient, since the outer call involves computation of hash of a short message.

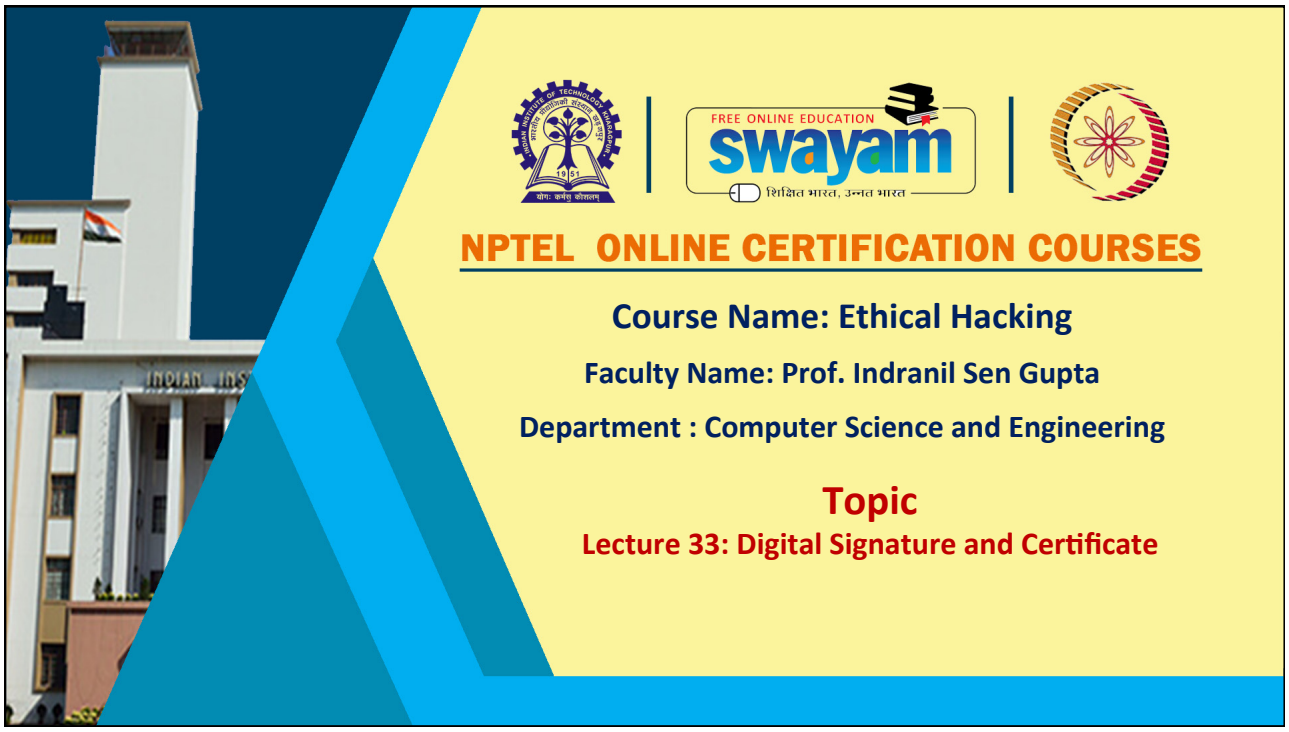

HMAC Structure



Hash Function: Attacks

- Birthday attack:
  - Let *H* be a hash function that produce *n*-bit hash values.
  - If about $2^{n/2}$ random messages are hashed by *H*, then it is highly probable that we have found two messages *x* and *x'* satisfying *H(x) = H(x')*.
  - The bit-size *n* of hash values should be at least 128. The values greater than or equal to 160 are recommended.
- Other attacks:
  - Attacks on the compression function.
  - Chaining attacks.
  - Attacks on the underlying block cipher.


FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
15



NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 33: Digital Signature and Certificate

CONCEPTS COVERED

- Digital signatures
- Digital certificates

Digital Signatures

Digital Signatures: Introduction

- Digital equivalent of hand-written signatures.
- Bind pieces of digital data with particular entities.
- Based on public-key technology.
- **Signing**:
  - The signer uses his private key *d* to sign.
- **Difficulty of forging:**
  - An entity without knowledge of this private key *d* cannot generate a valid signature on a new piece of data.

4

- **Verifying**:
  - Anybody having access to the signer's public key *e* can verify the signature.
- **Non-repudiation:**
  - An entity should not be allowed to deny valid signatures made by him.

Types of Digital Signatures

a) **Signature with appendix:** A representative *H(M)* of the message *M* is computed. A signing transformation f_s is applied on *H(M)*. Verification requires *M*.

- **Signature generation:**
  m = H(M)
  $s = f_s(m,d)$
  Output the signed message (M,s).
- **Signature verification:**
  Compute m = H(M)
  Compute $m' = f_v(s,e)$
  If (m = m') output "signature verified"
  else output "signature not verified"

Types of Digital Signatures (contd.)

b) Signature with message recovery: The signing transformation is applied to the message itself. The verification transformation retrieves the message.

- **Signature generation**:
  Compute the signature $s = f_s(M,d)$
- **Signature verification**:
  Recover the message $M' = f_v(s,e)$
  If M' looks like a valid message,
  output "signature verified"
  else
  output "signature not verified"


7

Types of Digital Signatures (contd.)

c) Deterministic signatures:

- For a given message the same signature is generated on every occasion the signing algorithm is executed.

d) Probabilistic signatures:

- On different runs of the signing algorithm different signatures are generated, even if the message remains the same.
- Offer better protection against some kinds of forgery.


8

Digital Signatures: Examples

- Rabin Signature
- ElGamal signature
- Schnorr signature
- Nyberg-Rueppel signature
- Digital signature algorithm (DSA)
- Elliptic curve version of DSA (ECDSA)
- XTR signature
- NTRUSign
- . . .


9

Digital Signatures: Blind Signatures

- The signer is not allowed to know the message to sign. Still his active participation is necessary for signing.
- **Blind RSA signature:**

  Signature generation:

  A generates a random integer k coprime to n.
  A blinds m as $m^* = mk^e \pmod n$.
  B signs $s^* = (m^*)^d \pmod n$.
  A retrieves B's signature $s = s^*k^{-1} \pmod n$.

  Signature verification: As before.


10

Digital Signatures: Undeniable Signatures

- An active participation of the signer is necessary during signature verification.
- A signer is not allowed to deny a legitimate signature made by him.
  - Non-repudiation.


Digital Signatures: Attacks

- **Total break:**
  - An attacker knows the signing key or has a function that is equivalent to the signature generation transformation.
- **Selective forgery:**
  - An attacker can generate signatures (without the participation of the legitimate signer) on a set of messages chosen by the attacker.
- **Existential forgery:**
  - The attacker can generate signatures on certain messages over which the attacker has no control.


Digital Signatures: Attacks

- **Key-only attack:**
  - The attacker knows only the verification (public) key of the signer. This is the most difficult attack to mount.
- **Known-message attack:**
  - The attacker knows some messages and the signatures of the signer on these messages.
- **(Adaptive) Chosen-message attack:**
  - This is similar to the known-message attack except that the messages for which the signatures are known are chosen by the attacker.


Digital Certificates


Digital Certificates: Introduction

- Bind public-keys to entities.
  - Required to establish the authenticity of public keys.
  - Guard against malicious public keys.
  - Promote confidence in using others' public keys.
- Require a *Certification Authority (CA)* whom every entity over a network can trust.
- In case a certificate is compromised, one requires to *revoke* it.
- A revoked certificate cannot be used to establish the authenticity of a public key.


Digital Certificates: Contents

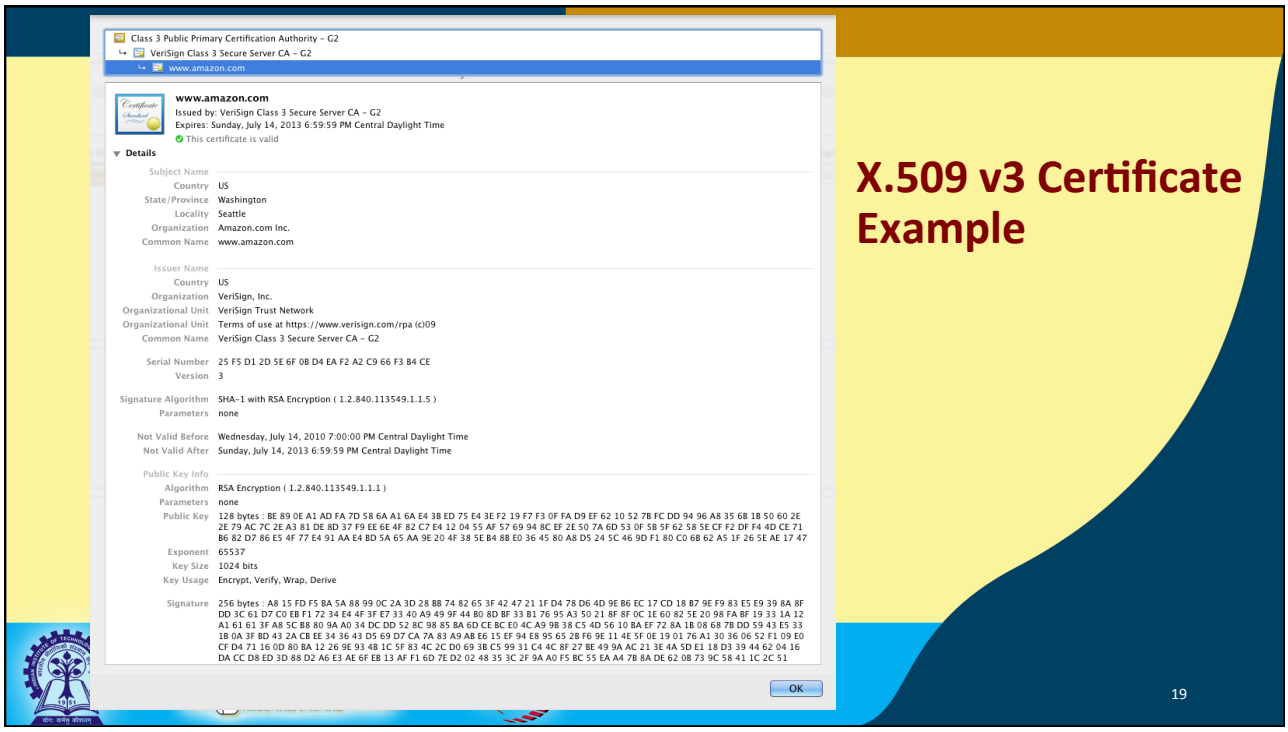
- A digital certificate contains particulars about the entity whose public key is to be embedded in the certificate. It contains:
  a) Name, address and other personal details of the entity.
  b) The public key of the entity.
- The certificate is digitally signed by the private key of the CA.
- If signatures are not forgeable, nobody other than the CA can generate a valid certificate for an entity.


Digital Certificates: Revocation

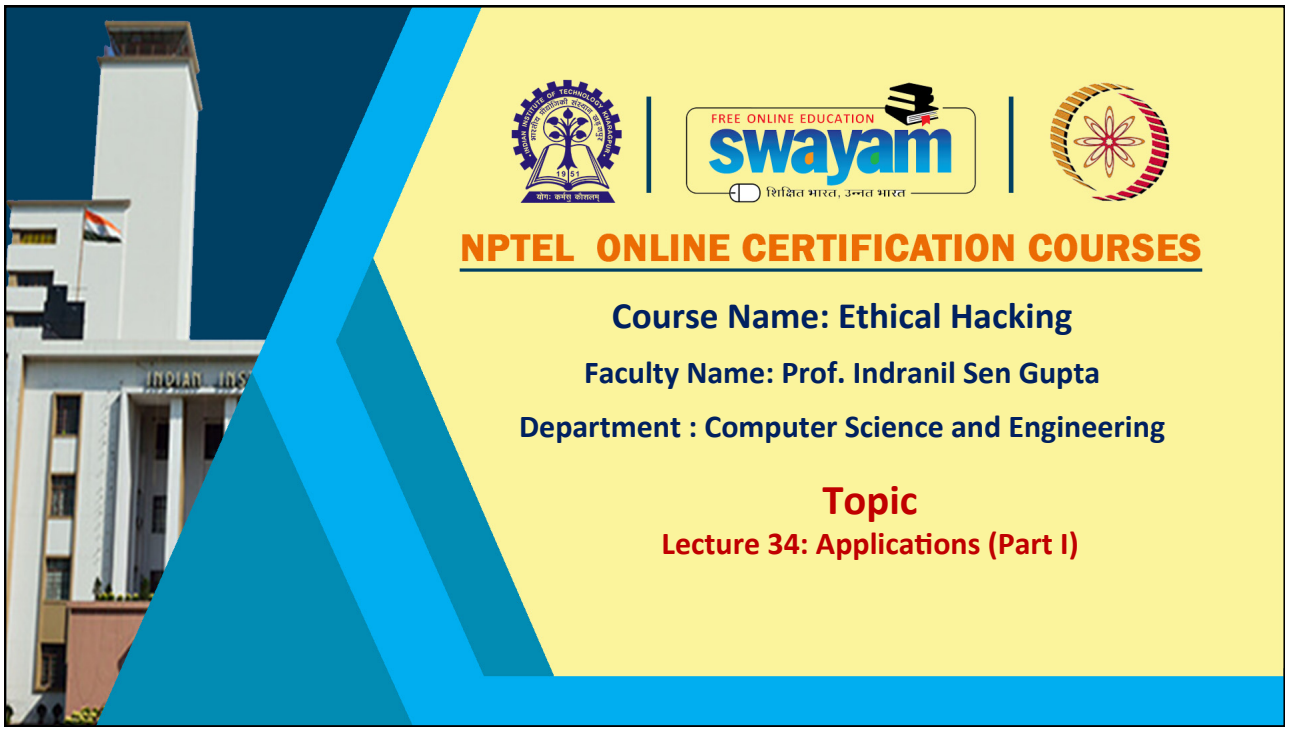
- A certificate may become *invalid* due to several reasons:
  - Expiry of the certificate.
  - Possible or suspected compromise of the entity's private key.
- An invalid certificate is *revoked* by the CA.
- The CA maintains a list of revoked certificates.
  - The Certificate Revocation List (CRL).


X.509 v3 Certificate Format

- Version
- Certificate Serial Number
- Signature Algorithm Identifier
- Issuer Name
- Validity Period
- Subject Name
- Subject Public Key Information
- Optional Fields



Class 3 Public Primary Certification Authority - G2
VeriSign Class 3 Secure Server CA - G2
www.amazon.com
www.amazon.com
Issued by: VeriSign Class 3 Secure Server CA - G2
Expires: Sunday, July 14, 2013 6:59:59 PM Central Daylight Time
This certificate is valid
Details
Subject Name
Country US
State/Province Washington
Locality Seattle
Organization Amazon.com Inc.
Common Name www.amazon.com
Issuer Name
Country US
Organization VeriSign, Inc.
Organizational Unit VeriSign Trust Network
Organizational Unit Terms of use at https://www.verisign.com/rpa (c)09
Common Name VeriSign Class 3 Secure Server CA - G2
Serial Number 25 F5 D1 2D 5E 6F 0B D4 EA F2 A2 C9 66 F3 B4 CE
Version 3
Signature Algorithm SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters none
Not Valid Before Wednesday, July 14, 2010 7:00:00 PM Central Daylight Time
Not Valid After Sunday, July 14, 2013 6:59:59 PM Central Daylight Time
Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters none
Public Key 128 bytes : BE 89 0E A1 AD FA 7D 58 6A A1 6A E4 3B ED 75 E4 3E F2 19 F7 F3 0F FA D9 EF 62 10 52 7B FC DD 94 96 A8 35 6B 18 50 60 2E 2E 79 AC 7C 2E A3 81 DE 8D 37 F9 EE 6E 4F 82 C7 E4 12 04 55 AF 57 69 94 8C EF 2E 50 7A 6D 53 0F 5B 5F 62 58 5E CF F2 DF F4 4D CE 71 B6 82 D7 86 E5 4F 77 E4 91 AA E4 BD 5A 65 AA 9E 20 4F 38 5E B4 8B E0 36 45 80 A8 D5 24 5C 46 9D F1 80 C0 6B 62 A5 1F 26 5E AE 17 47
Exponent 65537
Key Size 1024 bits
Key Usage Encrypt, Verify, Wrap, Derive
Signature 256 bytes : A8 15 FD F5 8A 5A 88 99 0C 2A 3D 28 8B 74 82 65 3F 42 47 21 1F D4 78 D6 4D 9E 86 EC 17 CD 18 B7 9E F9 83 E5 E9 39 8A 8F DD 3C 61 D7 C0 EB F1 72 34 E4 4F 3F E7 33 40 A9 49 9F 44 B0 8D BF 33 B1 76 95 A3 50 21 8F 8F 0C 1E 60 82 5E 20 98 FA BF 19 33 1A 12 A1 61 61 3F A8 5C B8 80 9A A0 34 DC DD 52 8C 98 85 BA 6D CE BC E0 4C A9 9B 38 C5 4D 56 10 8A EF 72 8A 1B 08 68 7B DD 59 43 E5 33 1B 0A 3F BD 43 2A CB EE 34 36 43 D5 69 D7 CA 7A 83 A9 AB E6 15 EF 94 E8 95 65 2B F6 9E 11 4E 5F 0E 19 01 76 A1 30 36 06 52 F1 09 E0 CF D4 71 16 0D 80 BA 12 26 9E 93 4B 1C 5F 83 4C 2C D0 69 3B C5 99 31 C4 4C 8F 27 BE 49 9A AC 21 3E 4A 5D E1 18 D3 39 44 62 04 16 DA CC D8 ED 3D 88 D2 A6 E3 AE 6F EB 13 AF F1 6D 7E D2 02 48 35 3C 2F 9A A0 F5 BC 55 EA A4 7B 8A DE 62 08 73 9C 58 41 1C 2C 51
OK
X.509 v3 Certificate Example
19


FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
20



NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 34: Applications (Part I)

CONCEPTS COVERED

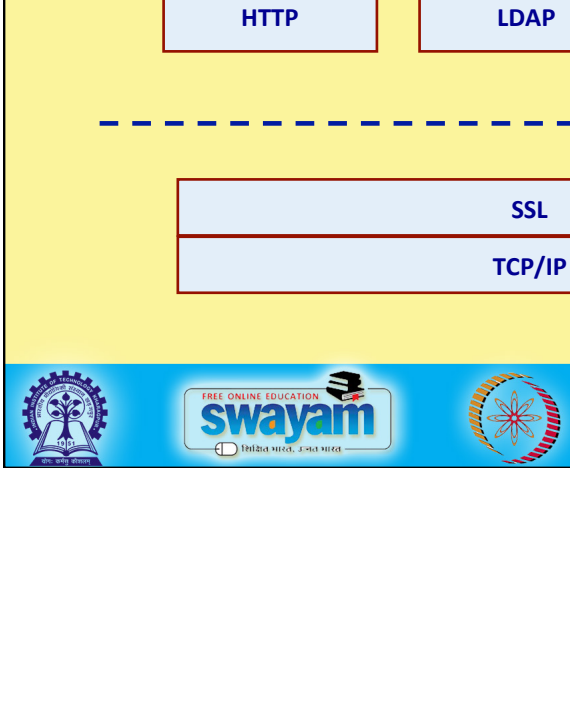
- Secure socket layer (SSL)
- How SSL works?

Secure Socket Layer (SSL)

Secure Socket Layer (SSL)

- SSL was first used by Netscape.
  - To ensure security of data sent through HTTP, LDAP or POP3.
- Uses TCP to provide reliable end-to-end secure service.
- In general, SSL can be used for secure data transfer for any network service running over TCP/IP.

- What is HTTP (Hyper-Text Transport Protocol)?
  - Protocol for communication between a web browser and a web server.
- What is LDAP (Lightweight Directory Access Protocol)?
  - An Internet directory service which is typically used by email systems to find more information about a user.
- What is POP3 (Post Office Protocol 3)?
  - A protocol using which email systems retrieve mails from the mail server.



Basic Objectives of SSL

- The main objectives are:
  a) Authenticate the client and server to each other.
  b) Ensure data integrity.
  c) Ensure data privacy
     - Required for both the protocol data and also the application data.


7

SSL Architecture

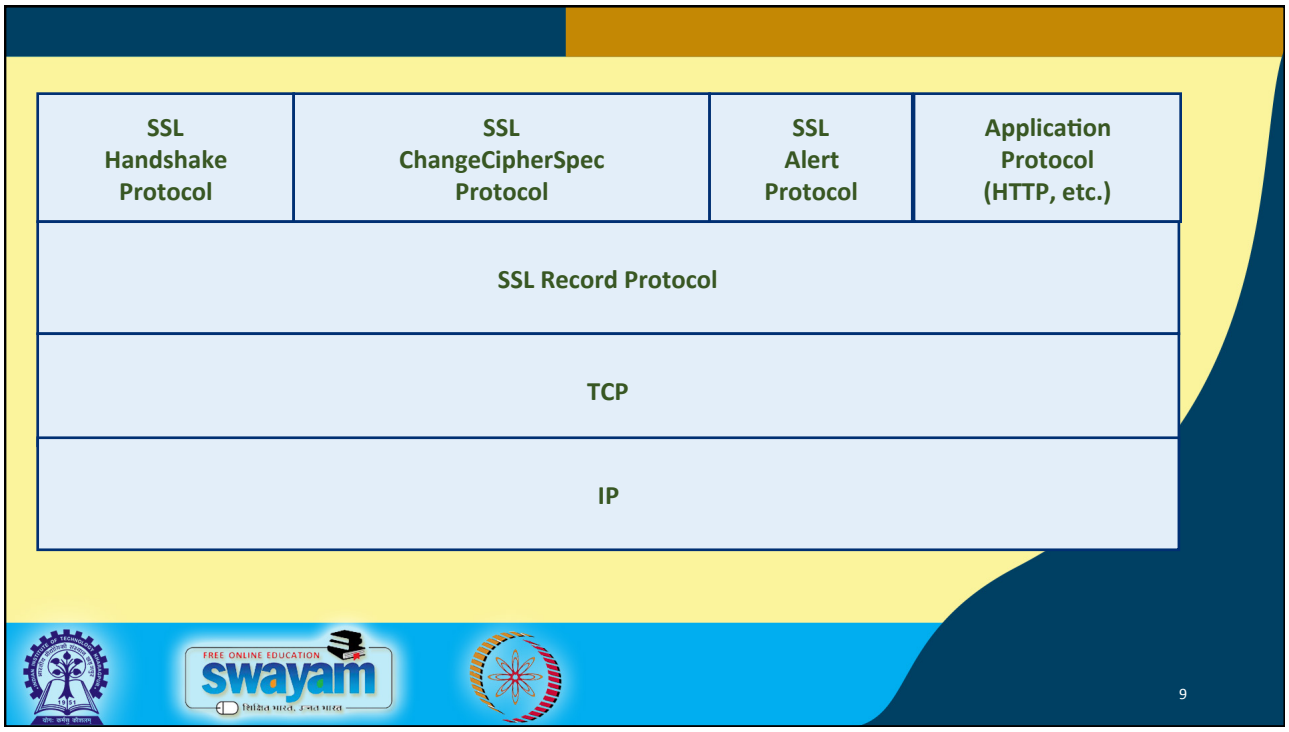
- SSL consists of two layers of protocols:
  a) SSL Record Protocol
     - Ensures data security and integrity.
  b) Protocols required to establish SSL connection.
     - Three protocols used in this layer:

       SSL Handshake Protocol

       SSL ChangeCipherSpec Protocol

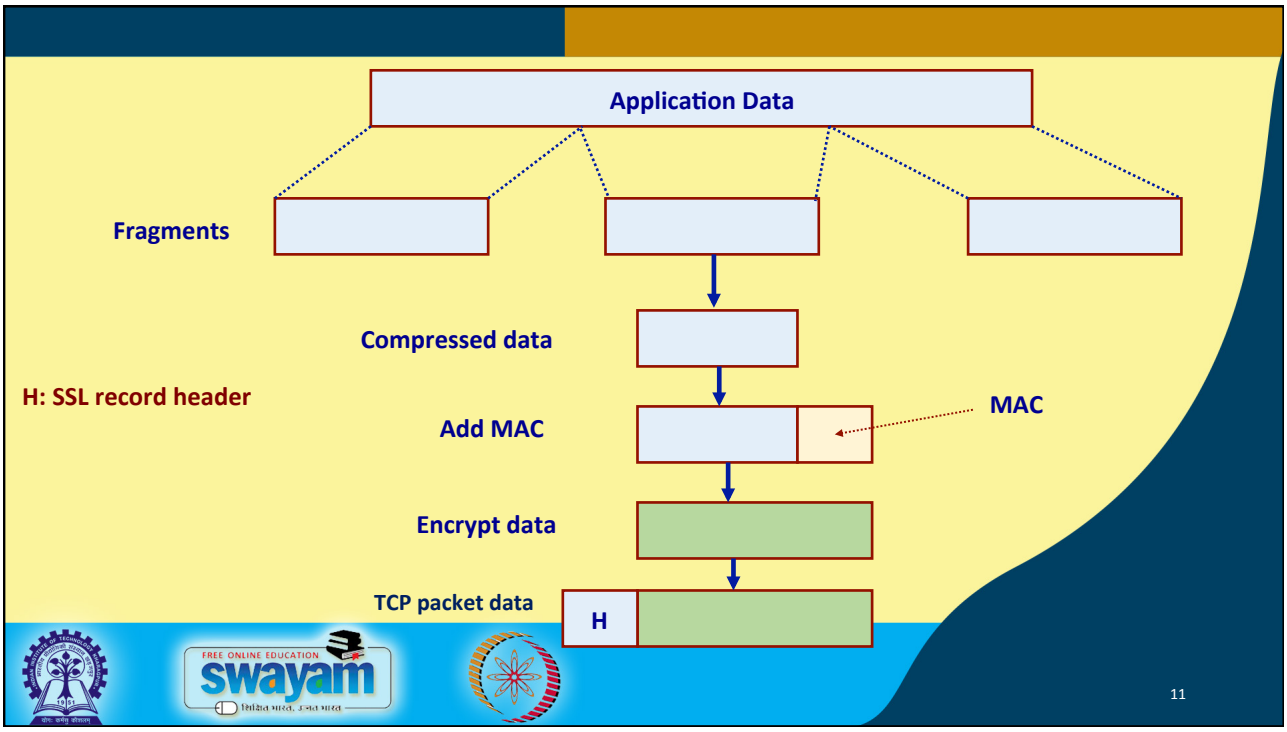
       SSL Alert Protocol


8



SSL Record Protocol

- Mainly responsible for data encryption and integrity.
  - Also used to encapsulate data sent by other higher level SSL protocols.
- Basic function:
  - Take an application message to be sent.
  - Fragment the application message data.
    - ❖ 16 Kbytes or smaller.
  - Encapsulate it with appropriate headers and create an object called a *record*.
  - Encrypt the record and forward it to TCP.



- SSL record header consists of:
  a) Content type:
     - identifies the type of payload (that is, the higher level protocol being used).
  b) Major version:
     - for SSL 3.0, the value is 3.
  c) Minor version:
     - for SSL 3.0, the value is 0.
  d) Compressed length:
     - size of the compressed data in bytes.

12

The Higher Layer Protocols

- **SSL Alert Protocol**
  - Used to send session messages associated with data exchange and functioning of the protocol.
  - Each message consists of two bytes:
    a) First byte is either 1 (warning) or 2 (fatal). If "fatal", the SSL session is terminated.
    b) Second byte contains one of the defined error codes.

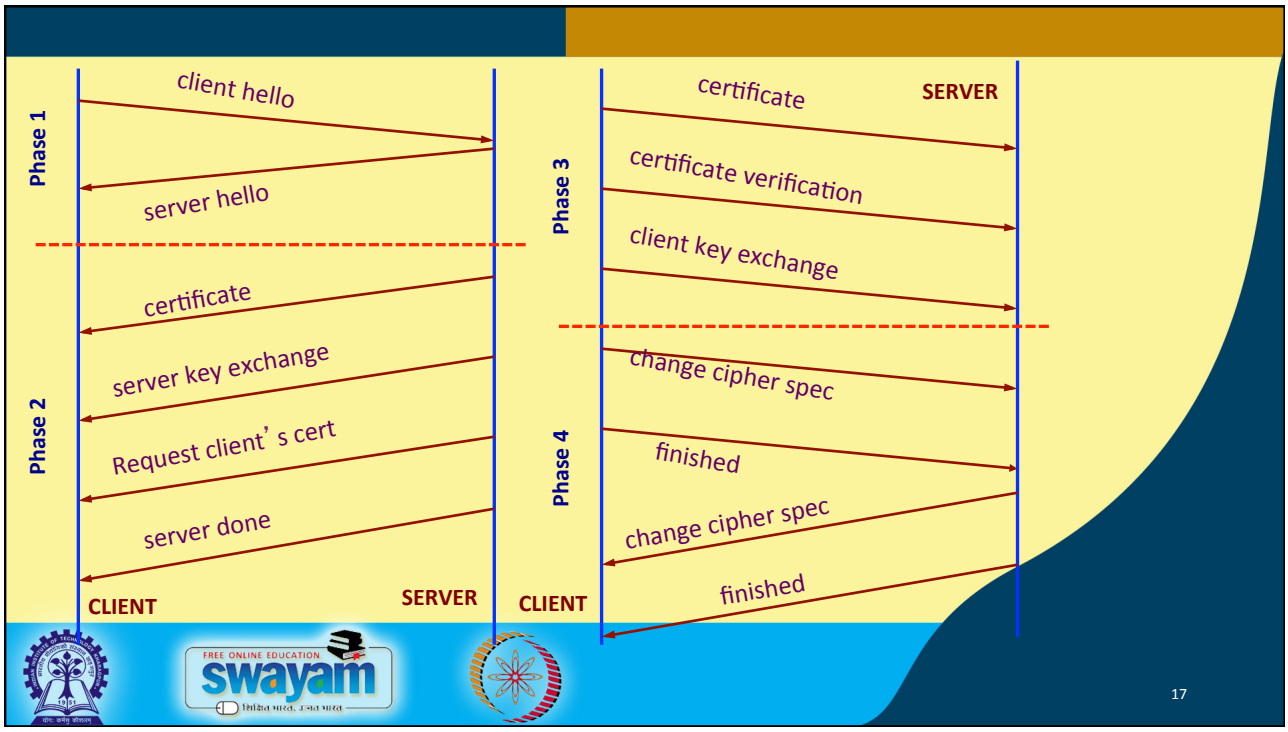

- **SSL ChangeCipherSpec Protocol**
  - Consists of a single message that carries the value of 1.
  - Purpose of this message is to cause the pending session state to be established as a fixed state.
    - ❖ Define the set of protocols to be used.
    - ❖ Must be sent from client to server, and vice versa.


- **SSL Handshake Protocol**
  - Used to initiate a session between the server and the client.
  - Within the application data, algorithms and keys used for data encryption can be negotiated.
  - Provides mutual authentication.
  - Process of negotiation divided into four phases.


15

- Client sends to the server
  - SSL version
  - Random (used to protect key exchange)
  - Session ID
  - CipherSuite
- Server sends back
  - SSL version
  - Random (a different number is generated)
  - Session ID
  - CipherSuite


16



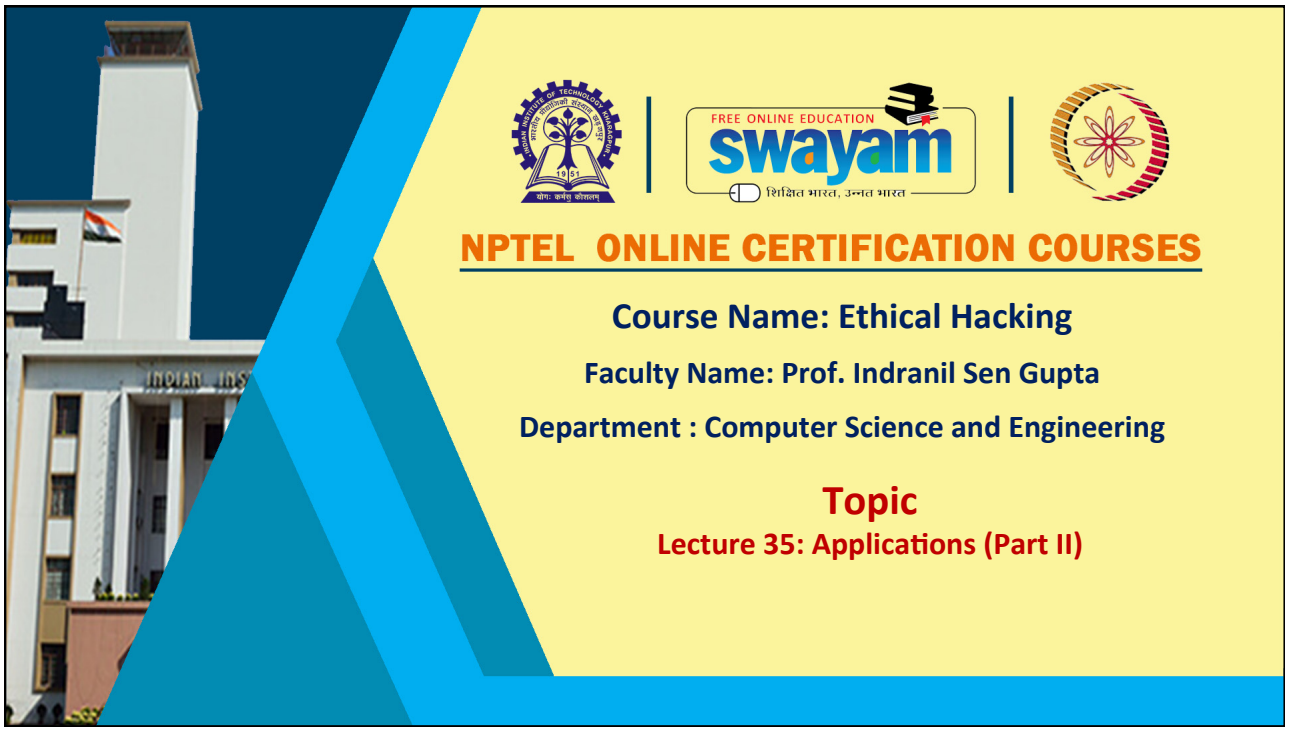
17

Some SSL Based Services

- HTTPS -- Port number 443
- LDAP -- Port number 646
- SMTP -- Port number 465
- POP3 -- Port number 995

18


FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
19



NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 35: Applications (Part II)

CONCEPTS COVERED

- Transport layer security
- IPSec
- S-HTTP

Transport Layer Security (TLS)

- Extension of SSL.
- Aim is to provide security and data integrity features at the transport layer between two web applications.
- Supported my most web servers and browsers today.


3

Secure Shell (SSH)


Introduction

- Originally developed in 1995.
  - As a secure replacement for telnet, rlogin, rcp, etc.
  - Allows port forwarding (tunneling over SSH)
  - Built-in support for proxies/firewalls.
- Widely used nowadays.


5

SSHv1 Protocol

- The server uses two keys:
  a) Long-term server identification key.
     - Binds the connection to the server.
     - 1024 bit RSA.
  b) Short-term encryption key, changed every hour.
     - Makes later recovery impossible.
     - Short-term keys are regenerated as a background task.
     - 768-bit RSA.


6

- Multiple authentication mechanisms
  - Straight passwords (protected by SSH encryption).
  - RSA based authentication.
    - Client decrypts a challenge from the server; returns the hash to the server.
  - Plug-in mechanisms (biometrics, smartcard, etc.).


7

IP Security (IPSec)


Introduction

- Security built into the IP layer.
  - Provides host-to-host (or firewall-to-firewall) encryption and authentication.
  - Required for IPv6, but optional for IPv4.
- Consists of two parts:
  - IPSec proper (for encryption and authentication).
  - IPSec key management.


9

IPSec

- Provides two modes of protection:
  a) Tunnel Mode
  b) Transport Mode
- Authentication and Integrity
- Confidentiality
- Replay Protection


10

(a) Tunnel Mode

- Encapsulates the entire IP packet within IPSec protection.
- Tunnels can be created between several different node types:
  - Firewall to firewall
  - Host to firewall
  - Host to host


11

(b) Transport Mode

- Encapsulates only the transport layer information within IPSec protection.
- Can only be created between host nodes.


12

Authentication and Integrity

- Verifies the origin of data.
- Assures that data sent is the data received.
- Assures that the network headers have not changed since the data was sent.


13

Confidentiality

- Encrypts data to protect against eavesdropping.
- Can hide data source when encryption is used over a tunnel.


14

Replay Prevention

- Causes retransmitted packets to be dropped.

Problems with IPSec

- Excessively complex and difficult to use.
- Does now allow use of NAT.
- Routers need to be made IPSec aware.

Secure HTTP (S-HTTP)

Introduction

- An extension to the HTTP protocol to support sending data securely over the web.
- Difference from SSL:
  - SSL is designed to establish a secure connection between two hosts.
  - s-HTTP is designed to send individual messages securely.

Some Features

- Provides a variety of security mechanisms to HTTP clients and servers.
- Does not require client-side public certificates (or public keys), as it supports symmetric key-only operation modes.
- Provides full flexibility of cryptographic algorithms, modes and parameters.


19

Point to Note

- s-HTTP and HTTPS are not the same.
- HTTPS is an alternative to s-HTTP.
  - HTTP runs on top of SSL or TSL for secured transactions.


20


FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
21