NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

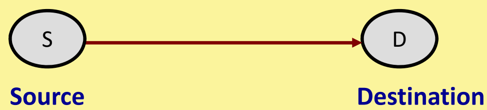
Lecture 26: Basic Concepts of Cryptography

CONCEPTS COVERED

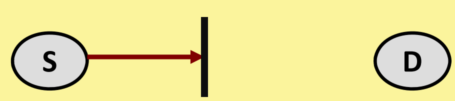
- Security attacks
- Security services
- Cryptographic primitives

Security Attacks

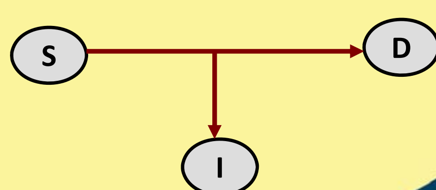
- Any action that compromises the security of information.
- Four types of attack:
    a) Interruption
    b) Interception
    c) Modification
    d) Fabrication
- Basic model:



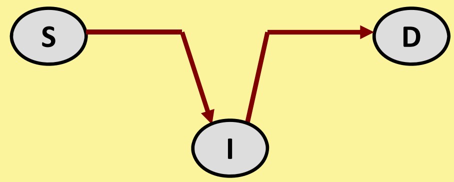
- Interruption:
    - Attack on availability



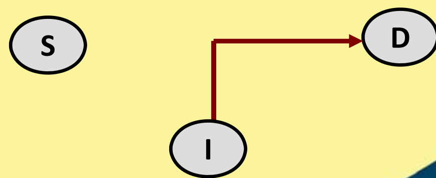
- Interception:
    - Attack on confidentiality



- Modification:
  - Attack on integrity



- Fabrication:
  - Attack on authenticity



Passive and Active Attacks

- **Passive attacks**
  - Obtain information that is being transmitted (eavesdropping).
  - Two types:
    a) Release of message contents.
    b) Traffic analysis.
  - Very difficult to detect.

- **Active attacks**
  - Involve some modification of the data stream or the creation of a false stream.
  - Four categories:
    - a) **Masquerade**:- One entity pretends to be a different entity.
    - b) **Replay**:- Passive capture of a transaction and subsequent replay.
    - c) **Modification**:- Some portion of a message is altered on its way.
    - d) **Denial of service**:- Prevents access to resources.

Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (parties cannot later deny)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

Network Access Security Model

Opponent:
- Human
- Virus
- Worm

ACCESS CHANNEL →

GATEWAY

Internal Network
- Computers
- Software resources
- Databases

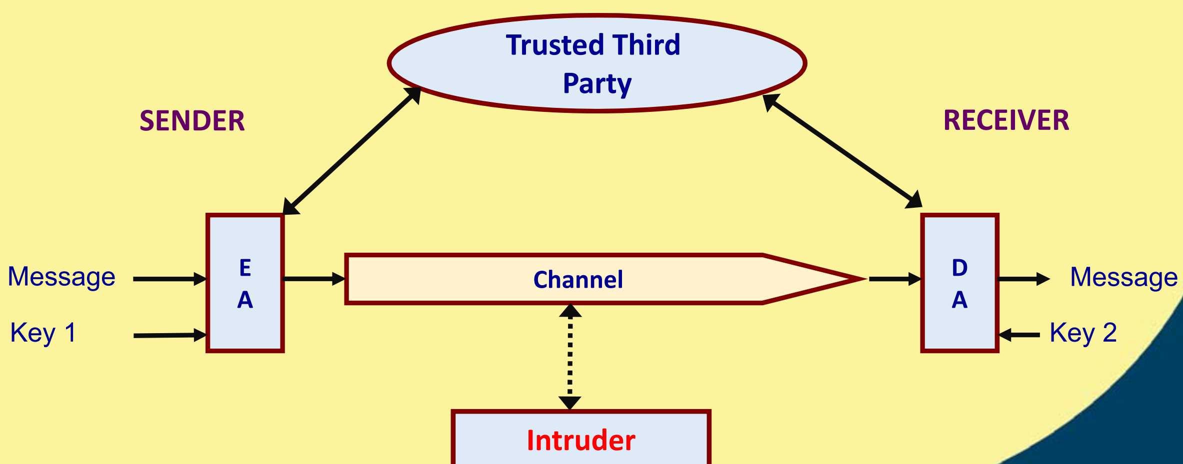
Security Control

Cryptography Primitives

Encryption

- Most important concept behind network security is *encryption*.
- Two forms of encryption:
  1. Private (or Symmetric)
     - Single key shared by sender and receiver.
  2. Public-key (or Asymmetric)
     - Separate keys for sender and receiver.

11



12

Authentication

- Techniques to uniquely identify the sender of a message.
- Various approaches:
  - Encryption techniques
  - Cryptographic hash functions
  - Digital signature → a combination of various cryptographic primitives.

13

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 27: Private-Key Cryptography (Part I)

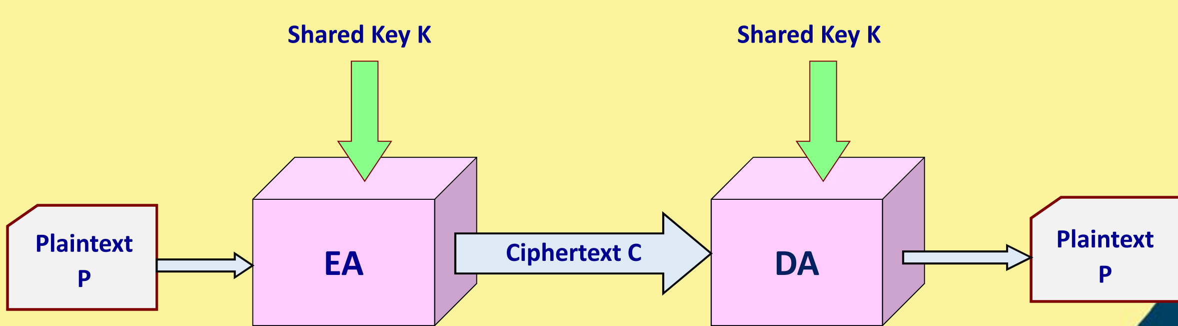
CONCEPTS COVERED

- Private/symmetric key cryptography
- Classical encryption techniques

Introduction

- Private or Symmetric Key Cryptography
  - A common secret value *K* (called ***key***) is shared between sender and receiver.
  - Sender encrypts a message *P* (called ***plaintext***) using *K* to generate a ***ciphertext*** *C*.
    - ❖ **C = EA (P, K)**
  - Receiver decrypts the ciphertext *C* using *K* to get back the plaintext *P*.
    - ❖ **P = DA (C, K)**

Illustration

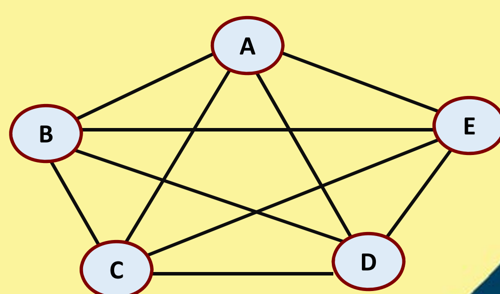


Point to Note

- Security of the scheme
  - Should depend only on the secrecy of the key.
  - Should not depend on the secrecy of the algorithm.
- Assumptions that we make:
  - Algorithms for encryption/decryption are known to the public.
  - Keys used for encryption/decryption are kept secret.

Some Points to Observe

- *Key distribution* problem of secret key systems:
  - Establish key before communication.
  - Need ***n(n-1)/2*** keys with ***n*** different parties.
- Overall, very large number of keys are required.
  - Difficult to maintain secrecy.



Classical Private-Key Encryption Techniques

- Broadly falls under two categories:
  1. **Substitution ciphers**
     - Each letter or group of letters of the plaintext are replaced by some other letter or group of letters, to obtain the ciphertext.
  2. **Transposition ciphers**
     - Letters of the plaintext are permuted in some form.

A Simple Example

Caesar Cipher (a substitution cipher):

- Earliest known substitution cipher.
- Replace each letter of the alphabet with the letter ***three places after*** that alphabet.
- Alphabets are assumed to be wrapped around (Z is followed by A, etc.).

P: H A P P Y N E W Y E A R

C: K D S S B Q H Z B H D U

- We can generalize the idea by replacing each letter by the k^{th} following letter.
  - "k" becomes the secret key.
- If we assign a number to each letter (A=1, B=2, etc), then

  C = E (P) = (P + k – 1) % 26 + 1

  P = D (C) = (C – k + 25) % 26 + 1

- **Drawback**:
  - Brute force attack is easy
  - Number of possibilities are rather small (i.e. 25)

9

Mono-alphabetic Cipher:

- Allow any arbitrary substitution.
- There can be 26! or 4 x 10^{26} possible keys.
- A typical key may be: (Z A Q W S X C D E R F V B G T Y H N M J U I K L O P)
  - "A" replaced by "Z", "B" replaced by "A", "C" replaced by "Q", and so on.
- Drawbacks:
  - We can make guesses by observing the relative frequency of letters, digrams, and trigrams in the text.
  - Easy to break in general.

10

Transposition Ciphers

- Many techniques have been proposed under this category.
- A simple scheme:
  - Write out the plaintext in a rectangle, row by row, and read the message column by column, by permuting the order of the columns.
  - Order of the column becomes the ***key***.

P: welcome to the nptel course on ethical hacking

Key:	4	3	1	2	5	6	7
	w	e	l	c	o	m	e
	-	t	o	-	t	h	e
	-	n	p	t	e	l	-
	c	o	u	r	s	e	-
	o	n	-	e	t	h	i
	c	a	l	-	h	a	c
	k	i	n	g	-	-	-

**C: lopu-ln c-tre-g etnonai w--cock otesth- mhleha-
ee--ic-**

Transposition Cipher … Drawbacks

- The ciphertext has the same letter frequency as the original plaintext.
- Guessing the number of columns and some probable words in the plaintext holds the key.

Practical Ciphers

- They are much more complicated.
  - Require computers to perform encryption and decryption.
  - Almost impossible to carry out by hand.
  - Can encrypt any kind of data, not necessarily only text.

Stream Ciphers vs. Block Ciphers

- A stream cipher encrypts the plaintext bit by bit (in streams).
- A block cipher encrypts n-bit blocks at a time.
  - For example, a 256-bit cipher encrypts 256-bit blocks at a time.
  - Shorter blocks have to be suitably padded.

15

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

16

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 28: Private-Key Cryptography (Part II)

CONCEPTS COVERED

- Practical private-key algorithms
- DES and Triple-DES
- Advanced Encryption Standard (AES)

Practical Private-Key Algorithms

a) Data Encryption Standard (DES)
  - Block size is 64 bits.
  - Key is 56 bits.

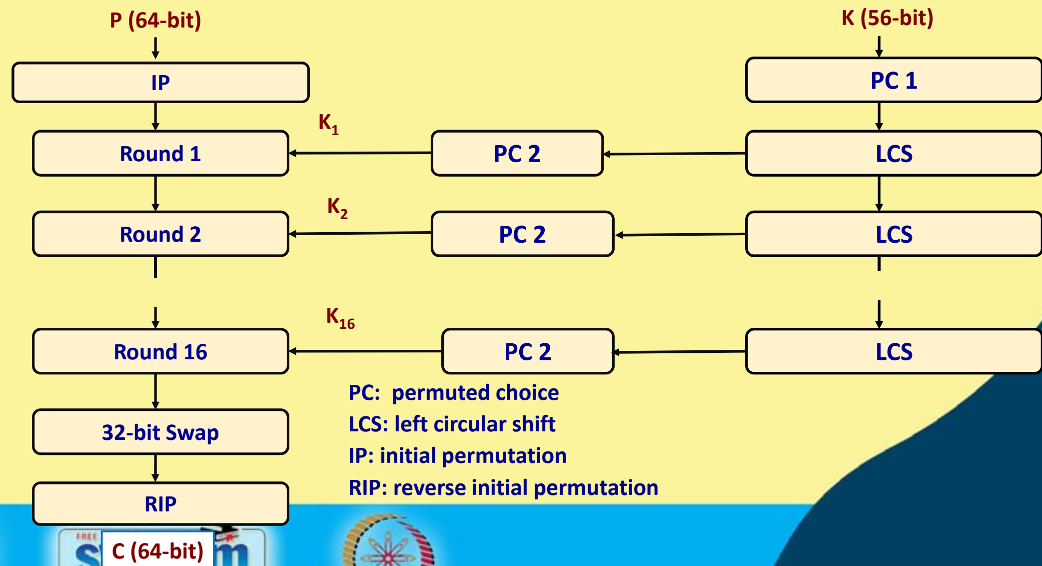
b) IDEA
  - Block size is 64 bits.
  - Key size is 128 bits.

c) Advanced Encryption Standard (AES)
  - Also known as Rijndael cryptosystem.
  - Block size is 128 bits.
  - Key size can be 128, 192, or 256 bits.

Data Encryption Standard (DES)

- The most widely used encryption scheme at one time.
  - Also known as the Data Encryption Algorithm (DEA).
  - It is a block cipher.
- Some of the features:
  - The plaintext is 64-bits in length.
  - The key is 56-bits in length.
  - Longer plaintexts are processed in 64-bit blocks.

General Schematic of DES



PC: permuted choice
LCS: left circular shift
IP: initial permutation
RIP: reverse initial permutation

DES

- The overall processing at each iteration:

$$\left.\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus F(R_{i-1}, K_i) \end{aligned}\right\} \textbf{Fiestel Structure}$$

- Concerns about:
  - The algorithm and the key length (56-bits).
  - Longer key lengths are essential for critical applications.

Triple DES

- Use three keys and three executions of the DES algorithm (encrypt-decrypt - encrypt).

$$C = E_{K3}\,[D_{K2}\,[E_{K1}\,[P]]]$$

C = ciphertext

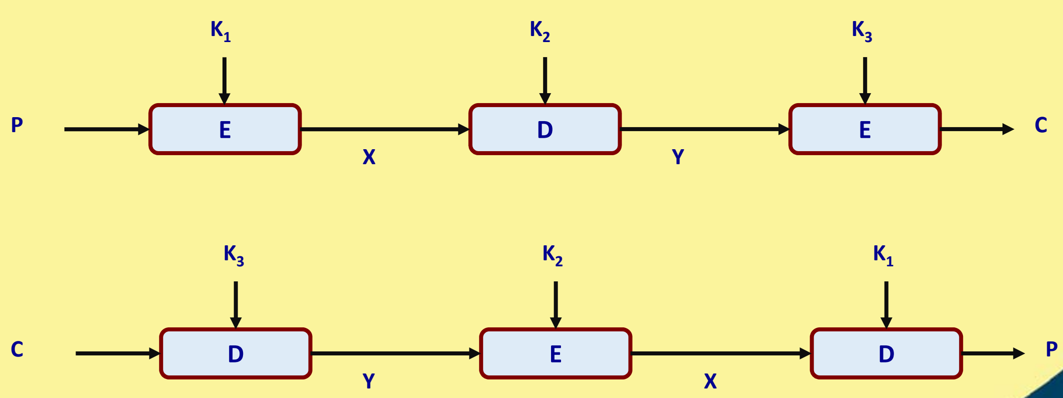
P = Plaintext

$E_K[X]$ = encryption of X using key K

$D_K[Y]$ = decryption of Y using key K

- Effective key length is 168 bits.

Triple DES: Illustration



Need for a new standard

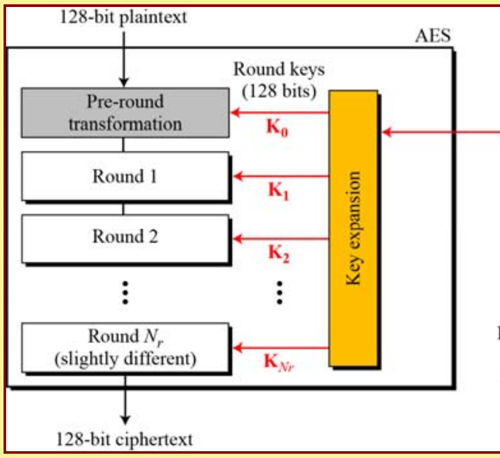
- DES had been in use for a long time.
  - A replacement for DES was needed.
  - Theoretical attacks can break it.
- Can use Triple-DES – but slow with small blocks.
- US NIST issued call for ciphers in 1997.
  - 15 candidates accepted in June 1998.
  - 5 were short-listed in August 1999.
- Rijndael was selected as the ***Advanced Encryption Standard*** in October 2000.

The AES Cryptosystem

- In the Rijndael proposal, the block length and the key length can be independently specified to be 128, 192, or 256 bits.
- The AES standard limits the block length to 128 bits.
  - Key length can be 128, 192, or 256 bits.
- Easy to implement, both in hardware and software.
- Resistant against all known attacks.

AES Rounds

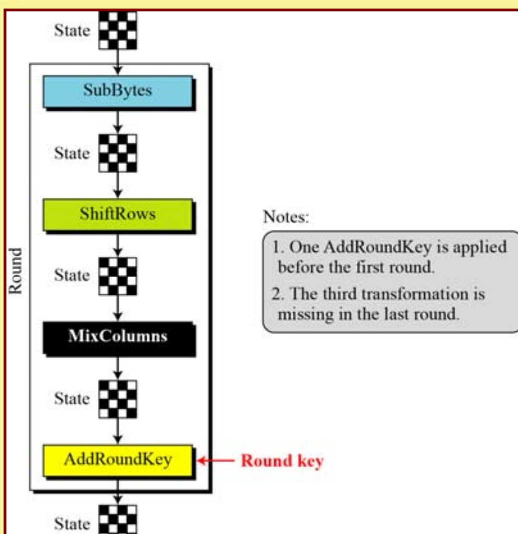
- AES has 10, 12 or 14 rounds.
  - All rounds are identical, except the first and last one.
- Various steps in each round:
  - **SubBytes** – Non-linear substitution
  - **ShiftRows** – Transposition
  - **MixColumn** – Mixing operations of each column
  - **AddRoundKey** – Round key added to state.

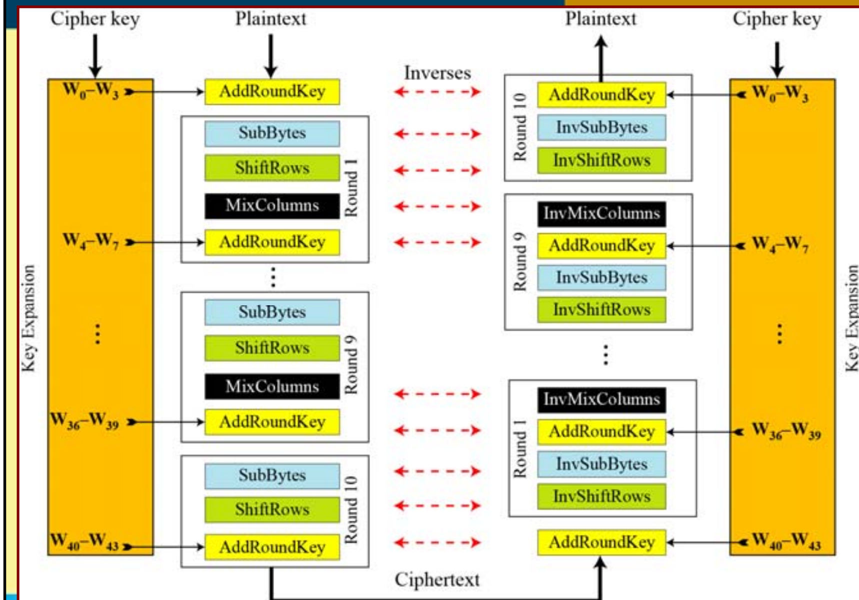


Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

Details of Each Round





Overall Structure

13

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

14

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 29: Public-Key Cryptography (Part I)

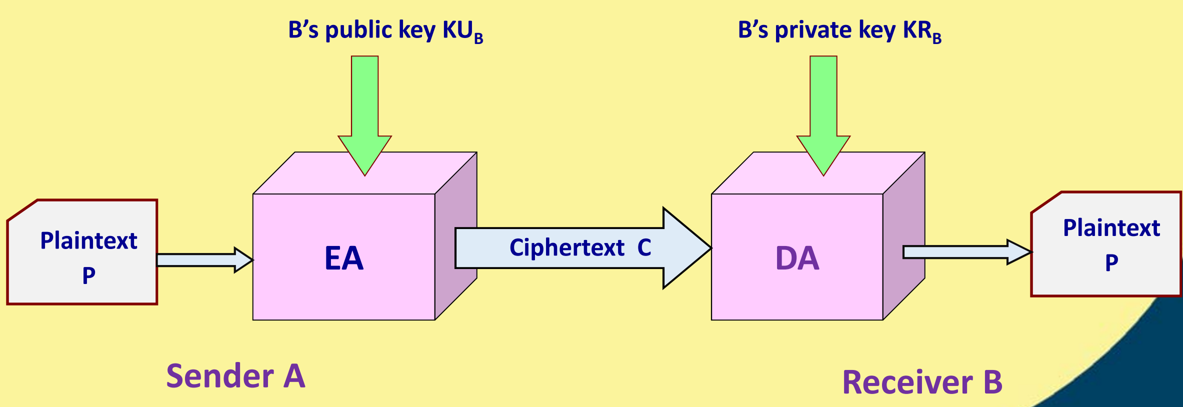
CONCEPTS COVERED

- Public-key cryptography
- Encryption and authentication
- RSA algorithm

Public Key Cryptography

- Uses two keys for every simplex logical communication link.
  a) Public key
  b) Private key
- The use of two keys has profound consequences in the areas of
  - Confidentiality
  - Key distribution
  - Authentication

Illustration :: Encryption



Key Usage for Encryption

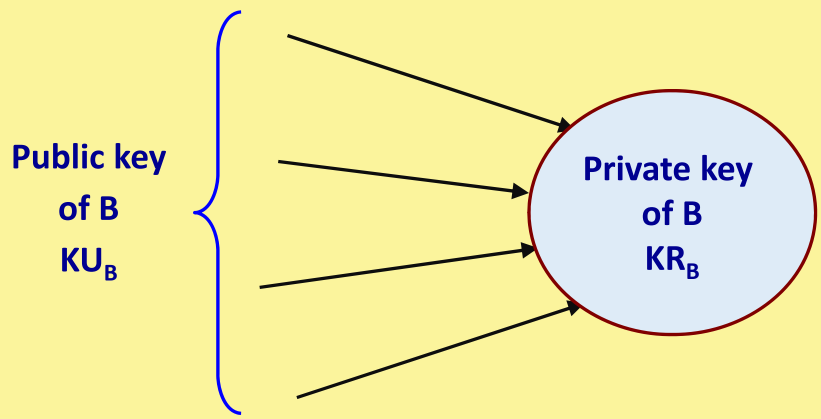
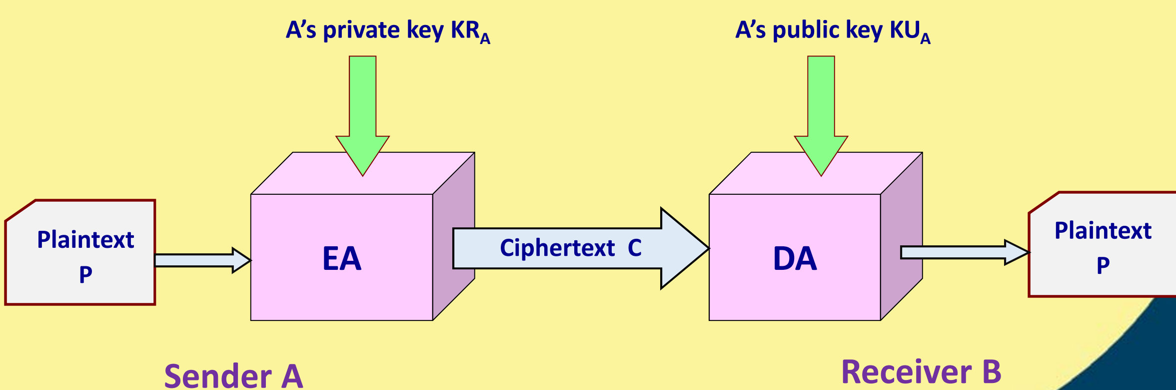
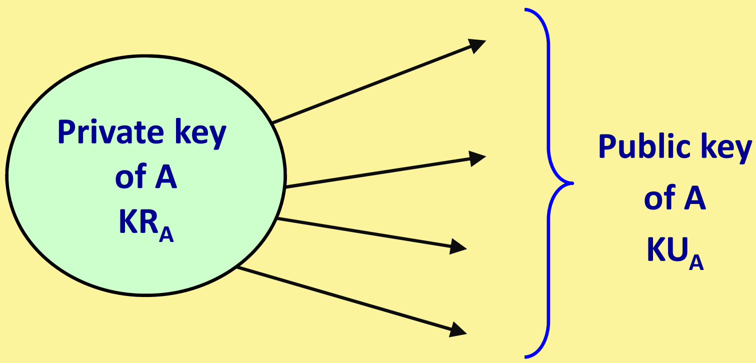


Illustration :: Authentication



Key Usage for Authentication



Applications

- Three categories:
  a) **Encryption/decryption:**
     - The sender encrypts a message with the recipient's public key.
  b) **Digital signature / authentication:**
     - The sender signs a message with its private key.
  c) **Key exchange:**
     - Two sides cooperate to exhange a session key.

Requirements

- Computationally easy for a party B to generate a key pair
  a) Public key KU_B
  b) Private key KR_B
- Easy for sender to generate ciphertext:

  $C = E(M, KU_B)$
- Easy for the receiver to decrypt ciphertext using private key:

  $M = D(C, KR_B) = D(E(M, KU_B), KR_B)$

- Computationally infeasible to determine **KR_B** knowing **KU_B**.
- Computationally infeasible to recover message **M**, knowing **KU_B** and ciphertext **C**.
- Either of the two keys can be used for encryption, with the other used for decryption:

  $M = D(E(M, KU_B), KR_B) = D(E(M, KR_B), KU_B)$

The RSA Public Key Algorithm

- RSA Algorithm
  - Developed by Ron Rivest, Adi Shamir and Len Adleman at MIT, in 1977.
  - A block cipher.
  - The most widely implemented.

RSA : Key Generation

1.	Select *p,q*	***p* and *q* both prime**
2.	Calculate $n = p \times q$	
3.	Calculate	$\Phi(n) = (p-1)(q-1)$
4.	Select integer *e*	$\gcd(\Phi(n),e)=1;\ 1<e<\Phi(n)$
5.	Calculate *d*	$d = e^{-1} \bmod \Phi(n)$
6.	Public Key	KU = {e,n}
7.	Private key	KR = {d,n}

$\phi(n)$ is the number of positive numbers less than *n* and relatively prime to *n* (called ***Euler totient***).

RSA : Encryption

- Plaintext: $M < n$
- Ciphertext: $C = M^e \pmod n$

RSA : Decryption

- Ciphertext: C
- Plaintext: $M = C^d \pmod n$

13

Example

- Select two prime numbers, p=7 and q=17.
- Calculate $n = pq = 7 \times 17 = 119$.
- Calculate $\phi(n) = (p-1)(q-1) = 96$.
- Select e such that e is relatively prime to $\phi(n)=96$, and less than $\phi(n)$.
  - In this case, e=5.
- Determine d such that $de = 1 \pmod{96}$ and $d<96$.
  - $d=77$, because $77 \times 5 = 385 = 4 \times 96+1$.

Public key KU = {5,119}
Private key KR = {77,119}

14

- **Encryption process:**
  - Say, plaintext M = 19.
  - Ciphertext C = 19^5 (mod 119)
    = 2476099 (mod 119) = 66
- **Decryption process:**
  - M = 66^{77} (mod 119) = 19.

The Security of RSA

- RSA is secure since
  - We use large number of bits in *e* and *d*.
  - The problem of factoring n into two prime factors is computationally very difficult.
    - ❖ Knowing *p* and *q* will allow us to know *Φ(n)*.
    - ❖ This will help an intruder to know the values of *e* and *d*.
  - Key sizes in the range of 1024 to 2048 bits seems safe.

Points to Note

- The RSA algorithm in conjunction with some private key algorithm (like AES) can be used for secure data transfer over insecure channel.
  - Private key K transmitted using public key algorithms (i.e. RSA).
  - K is used for encryption using private key algorithm.
- Prime factorization problem is solvable in polynomial time using quantum computers.
  - Resulted in research on post-quantum cryptographic algorithms.
  - Resistant against quantum attacks.

17

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

18

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 30: Public-Key Cryptography (Part II)

CONCEPTS COVERED

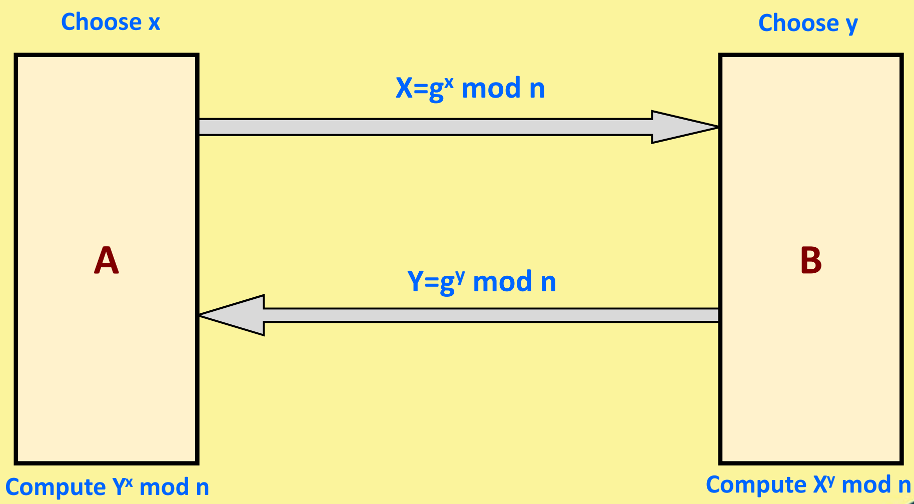
- ❑ Diffie Hellman key exchange
- ❑ Message authentication

Diffie-Hellman Key Exchange

- Proposed in 1976.
- Allows group of users to agree on secret key ***over insecure channel***.
- Cannot be used to encrypt and decrypt messages.
- Depends for its effectiveness on the difficulty of computing discrete logarithms.

D-H Algorithm

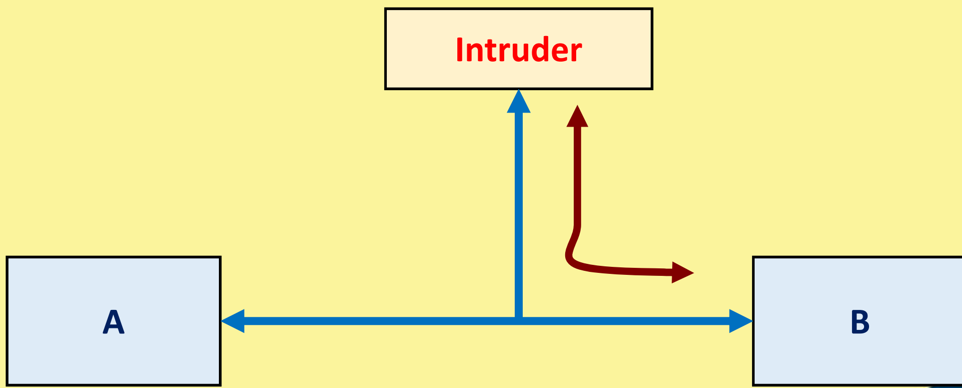
- A and B want to agree on secret key.
  - **a)** **A** and **B** agree on two large numbers **n** and **g**, such that $1<g<n$.
  - **b)** **A** choose random **x**, computes $X = g^x \bmod n$, and sends **X** to **B**.
  - **c)** **B** chooses random **y**, computes $Y = g^y \bmod n$, and sends **Y** to **A**.
  - **d)** **A** computes $k_1 = Y^x \bmod n$.
  - **e)** **B** computes $k_2 = X^y \bmod n$.
- Note: $k_1 = k_2 = g^{yx} \bmod n$.



D-H Algorithm (contd.)

- Requires no prior communication between ***A*** and ***B***.
- Security depends on difficulty of computing ***x***, given $X = g^x \bmod n$.
- Choices for ***g*** and ***n*** are critical.
  - Both ***n*** and ***(n-1)/2*** should be prime.
  - The value of ***n*** should be large.
- Susceptible to intruder-in-the-middle (man-in-the-middle) attack.
  - Active intruder.

Man-in-the-Middle Attack



A Comparison

- Symmetric encryption/decryption is much faster than asymmetric encryption/ decryption:

RSA: kilobits/second

DES: megabits/second

⇓

DES is about 100 times faster than RSA

- Key size:
  - a) **RSA**: selected by user
  - b) **DES**: 56 bits
  - c) **AES**: 128, 192 or 256 bits

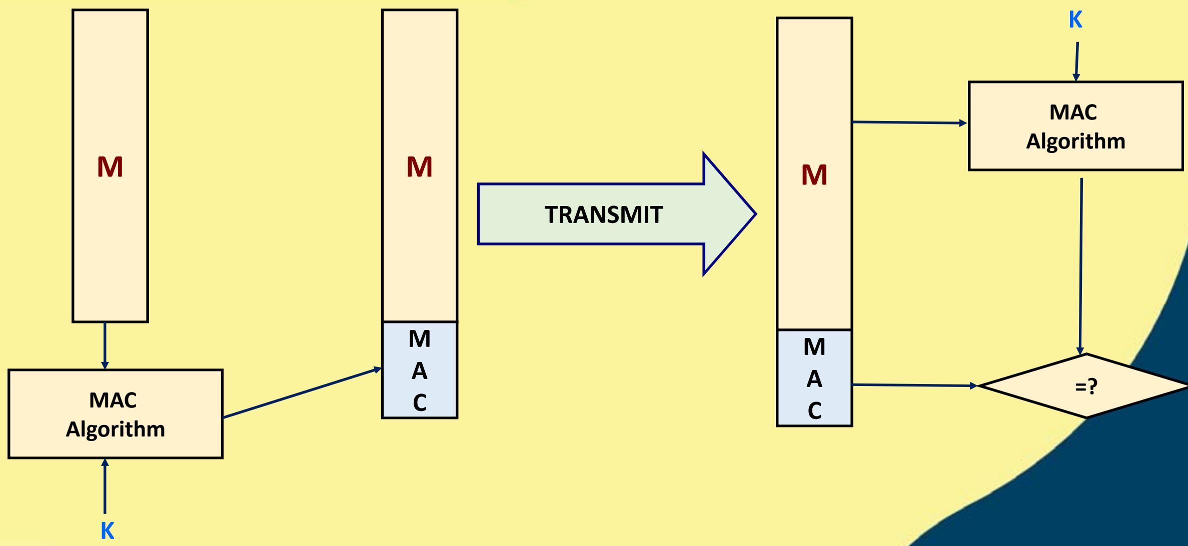
Message Authentication

Various Approaches

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)***



Commonly Used Schemes

- The MD family
  - MD2, MD4 and MD5 (128-bit hash).
- The SHA family
  - SHA-1 (160-bit), SHA-256 (256-bit), SHA-384 (384-bit) and SHA-512 (512-bit).
- RIPEMD-128 (128-bit), RIPEMD-160 (160-bit).


FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Thank you!