Security

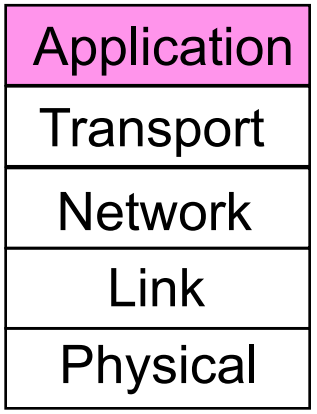
COMP90007

Internet Technologies

Chien Aun Chan

Outline: Network Security

- Network Security
- Cryptography
  - Basic Constituents and Relations
  - Ciphers
  - Algorithms



Security threats

Adversary	Goal
Student	To have fun snooping on people's email
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by email
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

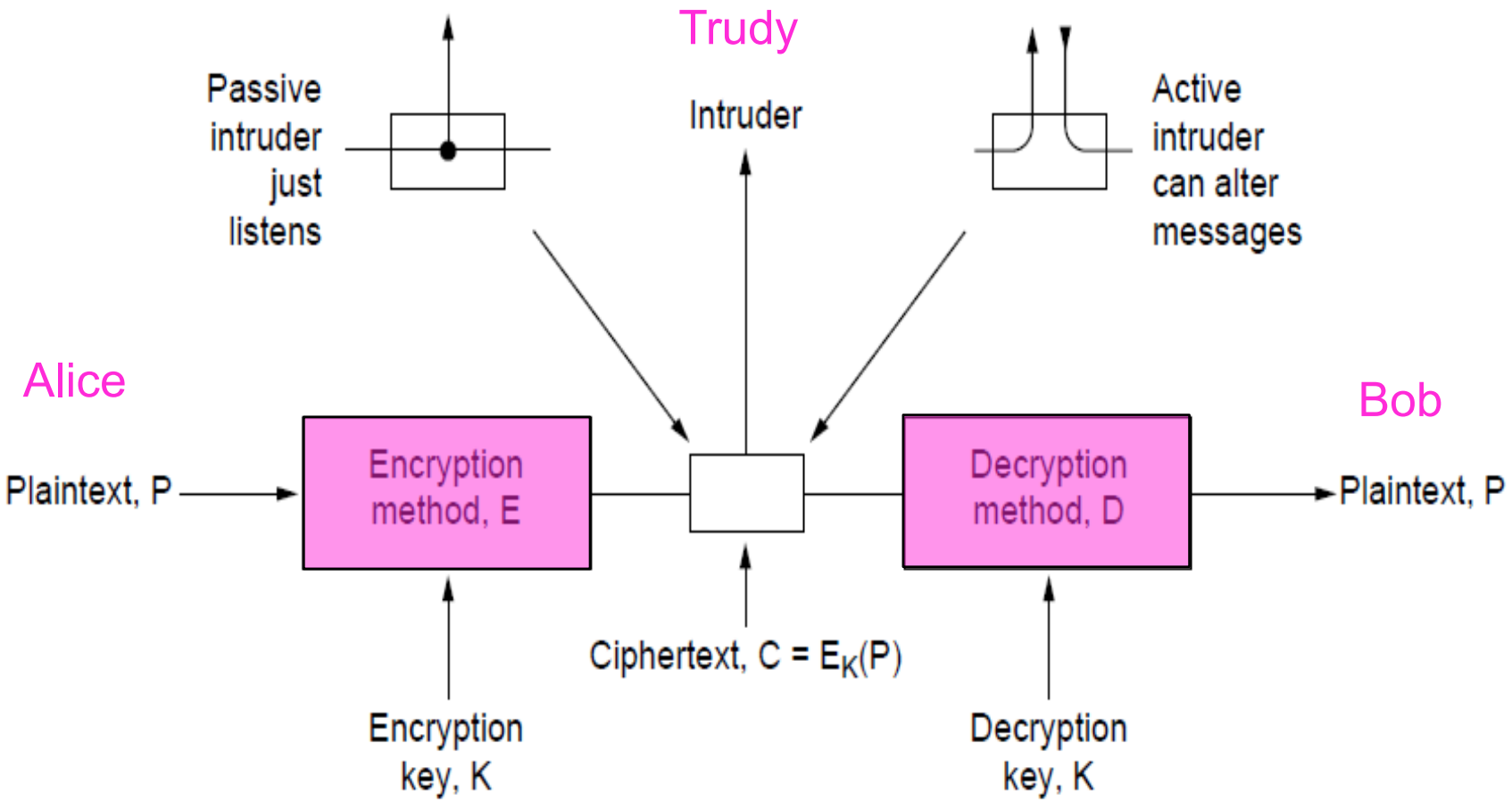
What is Security?

- Network security is a factor of 4 related concepts
  - Secrecy (Keeping information hidden from unauthorised users)
  - Authentication (Ensuring the user you are talking to has valid access to a given resource)
  - Non-repudiation (Prove a message was sent by a given user and it's contents are valid)
  - Integrity control (Ensure that a message has not been tampered with in transit)
- All of these are equally valid for traditional systems, but have different implications in a networked environment
- Aspects of security can be found at all layers of a protocol stack
- Apart from the physical layer, almost all security implementations are based on common cryptographic principles

Cryptography

- Cryptographic Constituents and Relations
- Symmetric Key Algorithms
- Assymetric Key Algorithms
- Digital Signatures
- Public Key Management

Encryption Model



Cryptography Concepts

- Three foundational concepts
  - Plaintext
  - Keys
  - Ciphertext
- Plaintext messages to be encrypted can be transformed (encrypted/decrypted) by a function that is parameterized by a key, the output of the transformation process is ciphertext
- Kerckhoff's principle: Cryptographic Algorithms and related functions (E, D) are public; only the keys (K) are secret

Relation of Cryptographic Constituents

- $C = E_K(P)$
- $P = D_K(C)$
- $D_K(E_K(P)) = P$
- Where: C = ciphertext, P = plaintext, E = encryption, D =decryption, K = key
- In fact what we require is
- $D_{K1}(E_{K2}(P)) = P$ if and only if k1=k2.

Keys Plays an Important Role

- A key is a short string that allows the selection of one of many potential encryptions
- The key can be changed as often as required
- How many possible keys are available when using numerical strings of length:
  - 2 digits?
  - 3 digits?
  - 6 digits?
- The size of the overall key space is determined by the number of bits in the key string
- The longer the key, the more effort is required to break a given encryption

Fundamental Machinery: XOR

- An XOR is an “exclusive or” function.
- A XOR B means A or B, but not both
- XOR is commonly used in cryptography as a comparison mechanism in multiphase encryption and decryption

A	B	A XOR B
F	F	F
F	T	T
T	F	T
T	T	F

Truth values	Binary Equivalents
T	1
F	0

Types of Ciphers

- Substitution cipher
  - Each letter of group of letters is replaced systematically by other letters or groups of letters (breakable with knowledge of the replacement system)
- Transposition cipher
  - All letters are re-ordered without disguising them (breakable with knowledge of re-ordering system)
- One-time pad
  - Uses a random bit string as the key, convert the plaintext into a bit string, then XOR the two strings bit by bit (unbreakable because any other plaintext has the same likelihood as the original message)

Substitution cipher

- Substitution ciphers replace each group of letters in the message with another group of letters based on a key with an intension to disguise the message.

plaintext:	a b c d e f g h i j k l m n o p q r s t u v w x y z
ciphertext:	Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

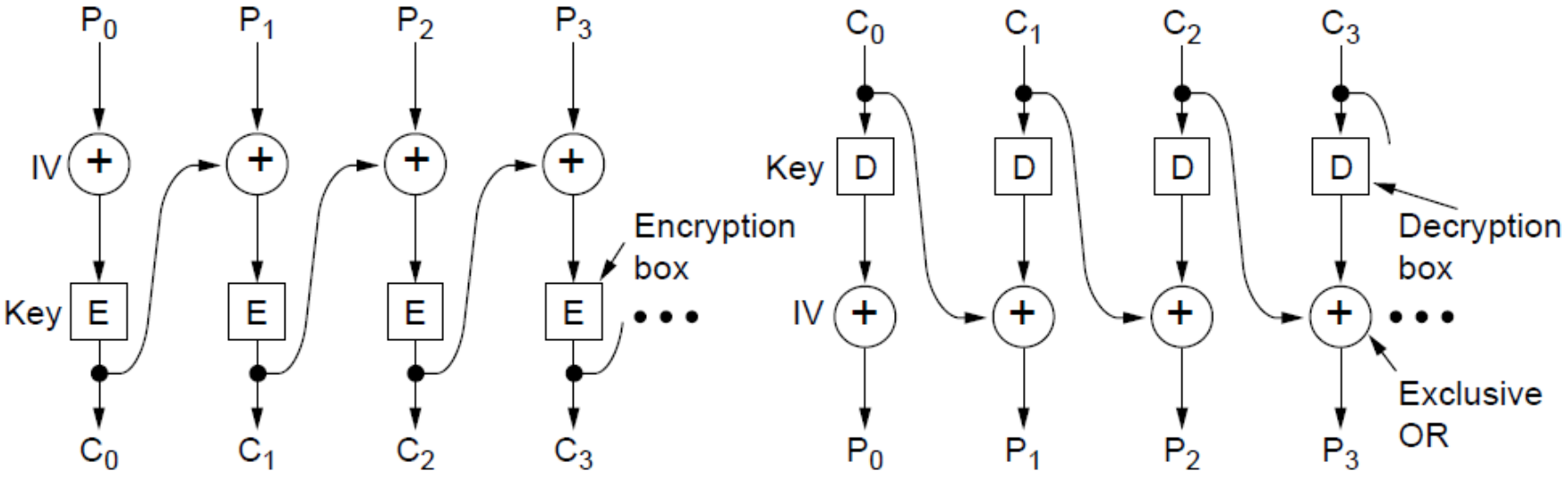
Symmetric Key Algorithms

- A symmetric key algorithm uses the same key for both encryption and decryption
- Symmetric key algorithms can use permutation, substitution and a combination of both to encrypt and decrypt
- 2 Symmetric Key Algorithms
  - Data Encryption Standard (DES)
    - Uses 64 bit blocks and 56 bit keys
    - 2^{56} key space
    - Triple DES has a 3 x 2^{56} key space
  - Advanced Encryption Standard (AES)
    - Uses 128 bit blocks and 128 bit keys (others available)
    - 2^{128} key space
- Electronic Code Book
  - Plain text → block cipher encryption → Ciphertext

Key →

Cipher Modes: Block Chaining

- In block chaining mode, each plaintext block is XOR'ed with the previous ciphertext block before being encrypted
- (a) encryption, (b) decryption

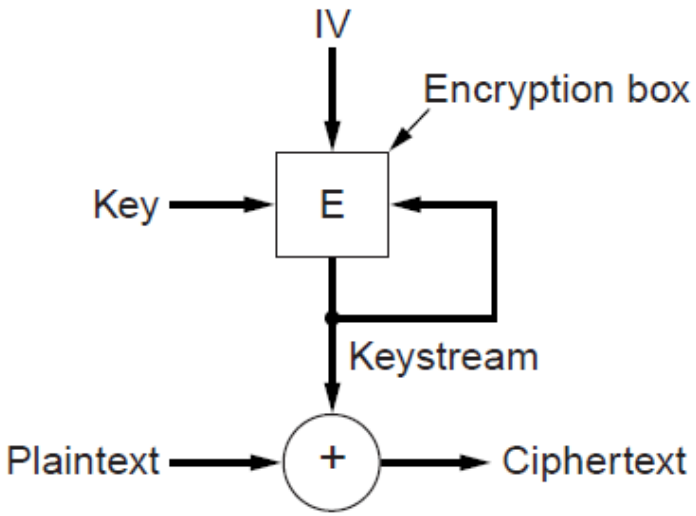


CBC mode encryption

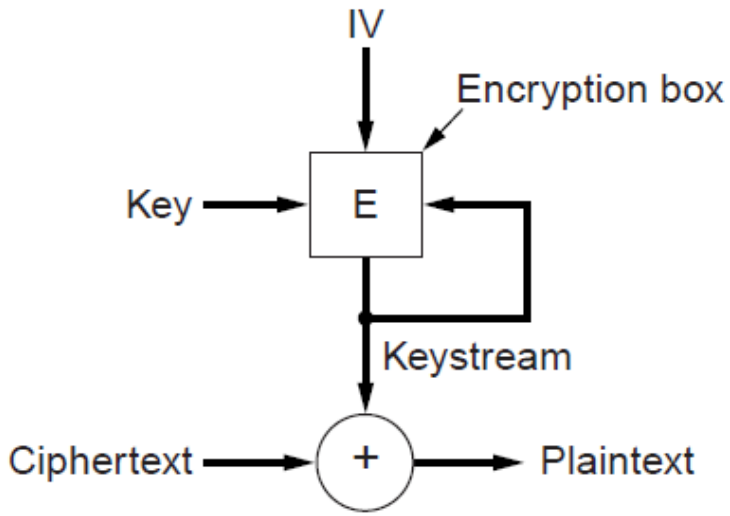
CBC mode decryption

Cipher Modes: Stream Ciphers

- In stream cipher mode, recursive sequential block encryption is used as a one-time pad, and XOR'ed with plaintext to generate ciphertext
- (a) encryption, (b) decryption



Encryption



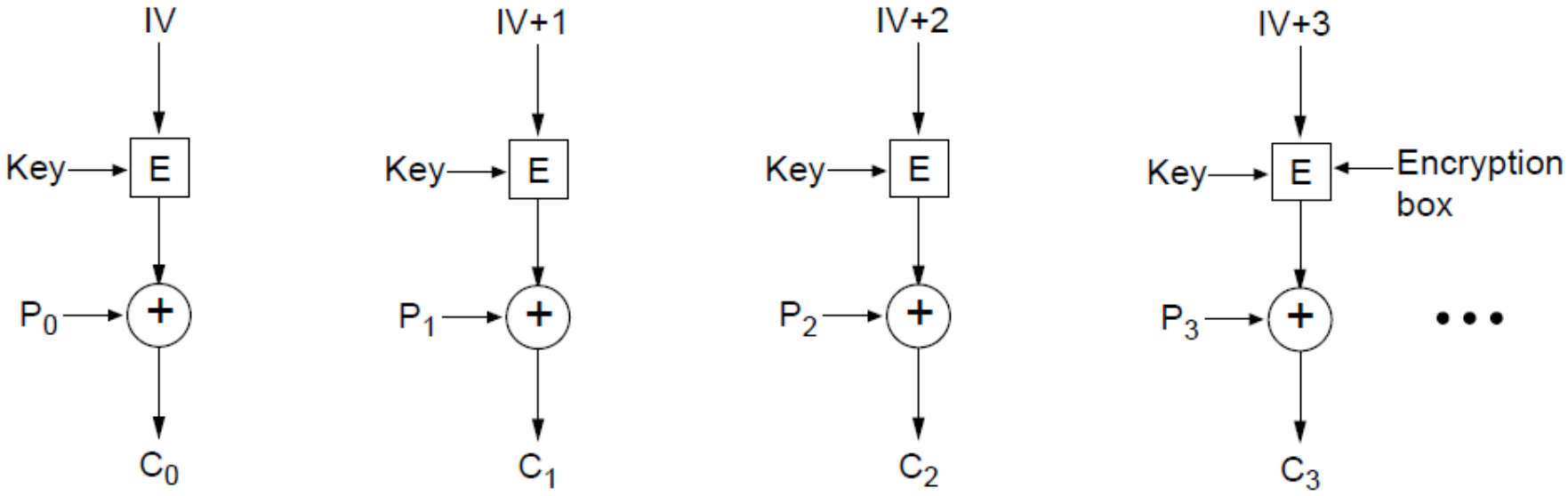
Decryption

Note:
C1 = A XOR K
C2 = B XOR K

C1 XOR C2 = A XOR B

Cipher Modes: Counter Mode

- In counter mode, plaintext is not directly encrypted, but an initialisation parameter plus an arbitrary constant is encrypted, and the resulting ciphertext is XOR'ed with plaintext to generate new ciphertext



Encryption above; repeat the operation to decrypt

Other Symmetric Key Algorithms

Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Public Key Algorithms

- Diffe & Hellman (1976) proposed a radically different model to symmetric key algorithms - asymmetric key algorithms, where the key used to encrypt and the key used to decrypt are different, and not derivable from each other
- Diffe-Hellman 2 key system
  - Key 1: public key, usable by anyone to encrypt messages to the owner of the key
  - Key 2: private key, required to decrypt the message (and held only by the owner of the key)

RSA, An Asymetric Key Algorithm

- RSA - Rivest, Shamir, Adleman (1978)
- Very robust algorithm, but requires keys of length 1024 bits
- Key generation:
  - Choose two large primes, p and q
  - Compute n = p × q and z = (p − 1) × (q − 1).
  - Choose d to be relatively prime to z
  - Find e to satisfy the *congruence relation* of e × d ≡ 1 mod z
    - Which means satisfy **(d x e) mod (z) = 1**
  - Public key is (e, n), and private key is (d, n)
- Encryption (of k bit message, for numbers up to n):
  - Cipher = $Plain^{e}$ (mod n)
- Decryption:
  - Plain = $Cipher^{d}$ (mod n)

RSA Security

- RSA's security is based on the difficulty involved in factoring large numbers - approx 10^{25} years to factor a 500 digit number using a brute force approach
- RSA is too slow for encrypting/decrypting large volumes of data, but is widely used for secure key distribution

RSA Example

- Let p=3, q=11 → n=33, z=20 → d=7, e=3

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Sender's computation

Receiver's computation

Encryption: $C = P^3 \bmod 33$

Decryption: $P = C^7 \bmod 33$

Using Cryptography: Digital Signatures

- Cryptographic approaches can be used to ensure authenticity and allow for non-repudiation
- Requirements
  - Receiver can verify the claimed identity of the sender
  - Sender cannot repudiate contents of the message
  - Receiver cannot have derived the message themselves
- Three approaches
  - Using symmetric keys via an intermediary to ensure non-repudiation
  - Using public keys as individuals
  - Using message digests

Message Digests

- Basic concept of a message digest is to use a one-way hash function to take an arbitrary length of plaintext and compute a fixed-length bit string
- A message digest (MD) has four important properties:
  - 1 Given P, it is easy to compute MD(P)
  - 2 Given MD(P) it is effectively impossible to find P
  - 3 Given P, no one can find P' such that MD(P') = MD(P)
  - 4 A change in even a single bit of input produces a very different output
- Given 3), the hashing function should be at least 128 bits long
- Given 4), the hashing function should scramble the bits very thoroughly
- Computing a message digest from plaintext is much faster than encrypting plaintext - so digests can be used to speedup the derivation of a digital signature

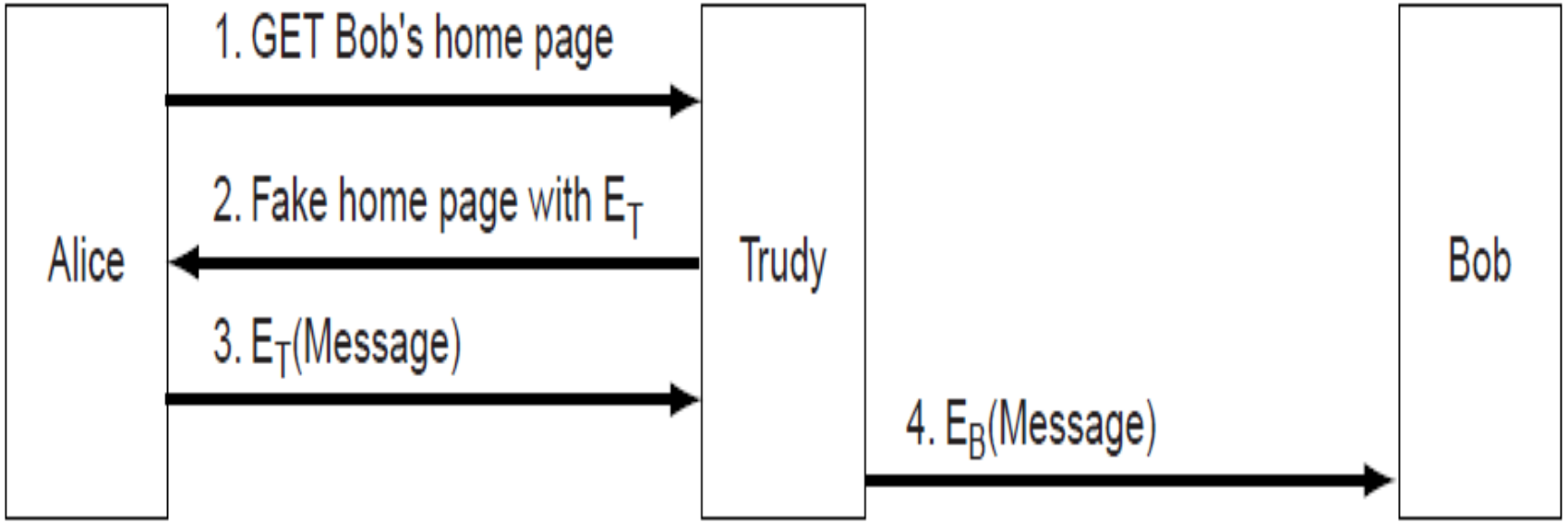
Message Digest Algorithms

- MD5
- Secure Hash Algorithm SHA-1
- Comparative output
  - File contents:\this is a test"
  - MD5: e19c1283c925b3206685522acfe3e6
  - SHA-1: 6476df3aac780622368173fe6e768a2edc3932c8

Public Key Management

- There is a need for specific PK infrastructure primarily to avoid compromising the security of PK's during the distribution process. We need a trusted way to distribute public keys.
- Certification Authority (CA)
  - A trusted intermediary who uses non-electronic identification to identify users prior to certifying keys and certificates
- X.509
  - An international standard for certificate expression
- PKI (Public Key Infrastructure)
  - Hierarchically structured certificate authorities allow for the establishment of a chain of trust or certification path

Management of Keys: Man in the middle



Trudy replaces E_B with E_T and
acts as a “man in the middle”

Outline

- Authentication
- Firewalls
- IPSec
- Virtual Private Network
- Wireless Security

Communication Network Security

- Cryptography provides the foundation on which network and application security operates

Authentication Protocols

- Authentication is a primary tenet of network security
- However, authentication itself needs to be secure also
- There are a number of common methods for secure authentication, but all subscribe to a single principle: minimise the use of permanent/private keys in establishment of secure connections (the less packets are exchanged using permanent/private keys, the less exposure to potential attackers)
- Four methods in common use:
  - Shared keys
  - Key distribution
  - Kerberos
  - Public keys

Authentication Protocols

- Four methods in common use:
  - Shared keys
    - one party sends a random number to the other party, who transforms it and sends the result back - essentially a challenge and response protocol
  - Key distribution
    - a trusted intermediary is used to facilitate the authentication
    - Users each share a key with a central key distribution centre, and authenticate to the KDC directly
    - The KDC then acts as a relay between the two parties
  - Kerberos
    - a multi-component system is required
      - Authentication Server
      - Ticket Granting Server
      - Recipient
    - Authentication is managed centrally, and then party to party communication is facilitated by single use cryptographic tickets
  - Public keys
    - Public Key Infrastructure with directory
    - Users enquire and get public keys of recipients from PKI for encryption containing sender identity

IPSec

- IPSec represents one view of how to embed security in the protocol stack - at the network level
- In the IPSec model, encryption is compulsory, but for graceful failover, a null encryption algorithm can be used between points which are not cryptographically inclined
- The major IPSec framework features are secrecy, data integrity, and replay attack protection
- The IPSec framework allows multiple algorithms and multiple levels of granularity
- IPSec is connection-oriented, with connections being called SA's (security associations)
  - SA includes attributes: cryptographic algo., cipher mode, traffic encryption key, etc..

IPSec Implementation

- IPSec has two main implementation components
  - New headers being added to packets in transit
  - ISAKMP key management
- IPSec has 2 modes
  - Transport mode - uses header insertion
    - Authentication Header (AH) - provides no data encryption but provides integrity checking using Hashed Message Authentication Code (HMAC) – for signature computation (hash over packet + shared key)
  - Tunnel mode - uses packet encapsulation
    - Encapsulating Security Payload (ESP) - provides an encryption layer as well as HMAC based integrity checking
    - Useful when a bundle of TCP connections is aggregated and handled as one encrypted stream – prevent intruder to see how many packets have been sent between two parties.

ISAKMP: Internet Security Association and Key Management Protocol

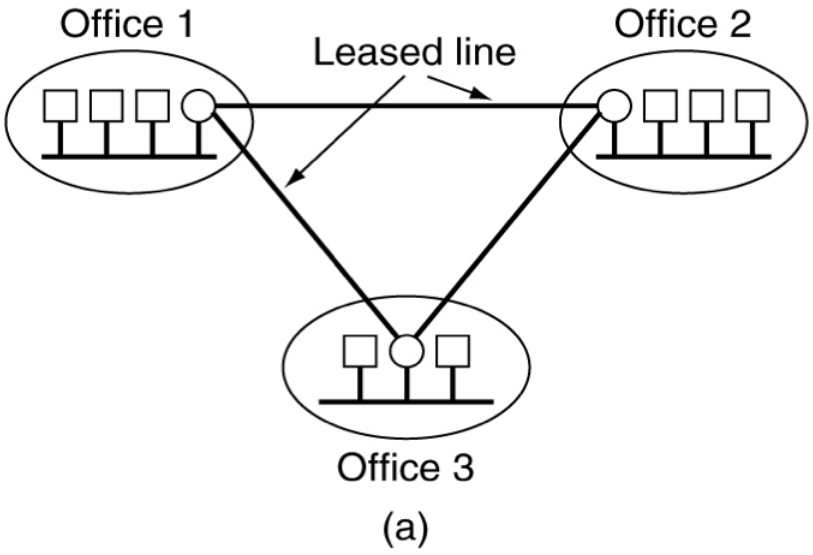
Virtual Private Networks

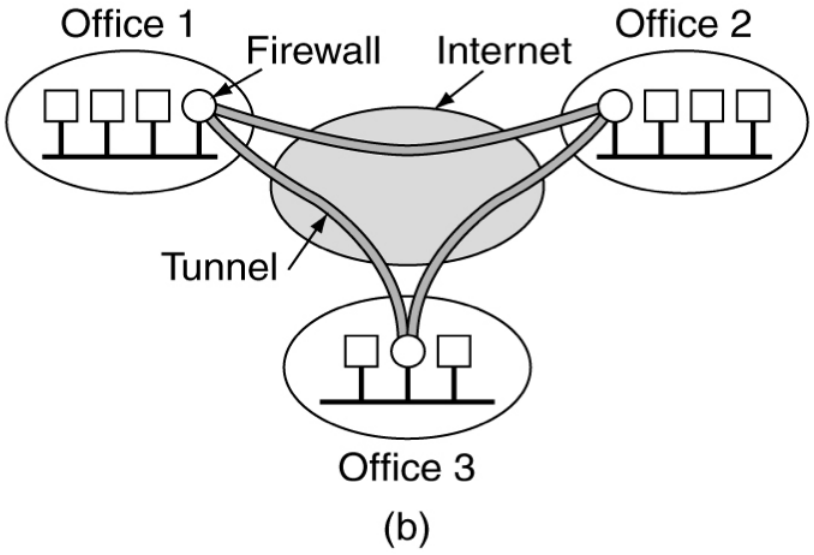
- Unlike a physical network based on leased lines between locations for which secure transit is required, a Virtual Private Network (VPN) is a virtual layer on top of an IP network which provides a secure end-to-end connection over public infrastructure
- A common VPN implementation model is to use a firewall at each end of a connection, use the firewalls to setup a SA to create an IPSec tunnel between the two end points, and then selectively route traffic for the specific destination via the encrypted connection
- Using such models, the security infrastructure is transparent to end users as the firewalls are responsible for the maintenance of the VPN

An SA is a simplex connection between two endpoints and has a security identifier associated with it

VPNs Illustrated

- (a) a leased line network
- (b) a virtual private network





IPSec VPNs

- Components of an IPSec VPN
  - Content encryption algorithm eg DES, 3DEs, AES
  - Collision-free hashing algorithm eg MD5, SHA-1
  - Diffie-Hellman key exchange protocol
  - Public Key Infrastructure for Certification
- IPSec VPN Architecture
  - Authentication Header (AH) added to an IP Packet to provide data origin authentication and data integrity checking
  - An Encapsulating Security Payload (ESP) for IP provides encryption, data origin authentication and data integrity checking
- Internet Security Association and Key Management Protocol (ISAKMP) and Internet Key Exchange (IKE) allow VPN devices to
  - securely negotiate and manage IPSec security associations (SAs)
  - to generate, exchange and manage the keys that are used by the cryptographic algorithms employed by IPSec

Firewalls

- While IPSec ensures security in transit, a firewall ensures security at the network perimeter
- Firewalls are positioned at the network boundary, and provide a controlled series of route between the internal and external networks
- Three characteristics of firewalls
- All inbound and outbound traffic must transit the firewall
- Only authorised traffic must pass through the firewall
- Firewalls should be immune to penetration themselves

Firewall Scope

- Single choke point for range of functions
  - Deny access to unauthorised users either inbound or outbound
- Monitoring location for security related events
- Platform for non-security functions
  - NAT
  - Usage logging and auditing
- Platform for extended security functions
  - IPSEC
  - VPNs
  - Anti-Virus

Firewall Constraints

- No protection against threats originating via bypass networks
  - Direct dialin systems
  - Direct dialout systems
- No protection against internal threats
  - Network segmentation and access control may alleviate internal risks
- No protection against application payload threats
  - Viruses, Trojans etc spread as application payloads eg email attachments

Wireless Security Context

- Wired networks are relatively easy to secure because they require physical access to intercept traffic
- Wireless networks are more difficult to secure because of omnidirectional signal propagation
- Additionally by default most wireless network equipment operates in an insecure and promiscuous manner
- 802.11 has a native secure protocol, Wired Equivalency Protocol (WEP), which is a 40-bit encryption based on RC4 algorithm

Wireless Security Issues

- WEP users from two inherent insecurities
  - 40 bit encryption is breakable with low-moderate computational resources
  - RC4 re-uses keys, so capturing a small volume of encrypted traffic will guarantee key identification
    - An inherent weakness in WEP is that it uses only a 24 bit range to populate initialisation values for RC4, so after 2^{24} packets, the sequence cycles being to repeat
    - A number of attacks against RC4 have demonstrated that the key can be derived from the encrypted stream given sufficient sample data
- Given these constraints, how can wireless networks be secured ?

Securing Wireless

- MAC Address Filtering
  - Only allow specified MAC interfaces to establish connections
- Non-Broadcast SSID
  - Prevent discovery of Community String by eavesdroppers
- Additional encryption (128bit WEP)
  - Increased security through longer key lengths
- WPA (WiFi Protected Access 2)
- Multilayered security
  - All of the above plus a VPN over wireless and regimented user authentication

SSID: Service Set Identifier

Summary - Security

- Cryptography
  - Contrast the strengths and weaknesses of different cipher modes
  - Explain the use of message digests
- Authentication
  - Describe the basic operation of authentication using public key cryptography
- Network Security
  - Describe the key functions that need to be provided by a firewall
- Summarise some of the challenges for wireless network security