



## Network Security

### Security Fundamentals

- **Attacks on Internet** (Self Reading)
- Services by a Security System (Fast Review)
- Security protocols and algorithms (Fast Review)
- Internet Security Practices and Examples  
IPsec, TLS, PGP, VPN...

**Dr. Anand Bhojan**

COM3-02-49, School of Computing

[banand@comp.nus.edu.sg](mailto:banand@comp.nus.edu.sg) ph: 651-67351

# Threats to Lives?

## Dutch hacking attack grave threat to Iranian dissidents

Published on : 5 September 2011 - 6:35pm | By Erik Klooster (Photo: RNW)

More about: certificates of authenticity Diginotar Holland Iran Iranian censorship Iranian dissidents Netherlands

**Iranian dissidents are at grave risk after hackers broke into a Dutch internet company, allowing the Iranian authorities to read messages sent through normally secure sites such as Yahoo and Gmail.**

**Who issues certificates of authenticity?**

Before the breach, DigiNotar was



damage to the nuclear program of Iran.  
Target - SCADA system.

## Hackers 'hit' US water treatment systems

Hackers are alleged to have destroyed a pump used to pipe water to thousands of homes in a US city in Illinois.

Hackers with access to the utility's network are thought to have broken the pump by turning it on and off quickly.

The FBI and Department for Homeland Security (DHS) are investigating the incident as details emerge of what could be a separate second attack.



GETTY IMAGES

Source: Rnw, BBC

# Underground Economy



Hack



Sell Services



Bank account with \$200K sold  
Own a Machine for \$0.40  
\$\$\$ for Installing Malware  
E-passports for \$12  
Configure your malware!  
Click Fraud, Spam services

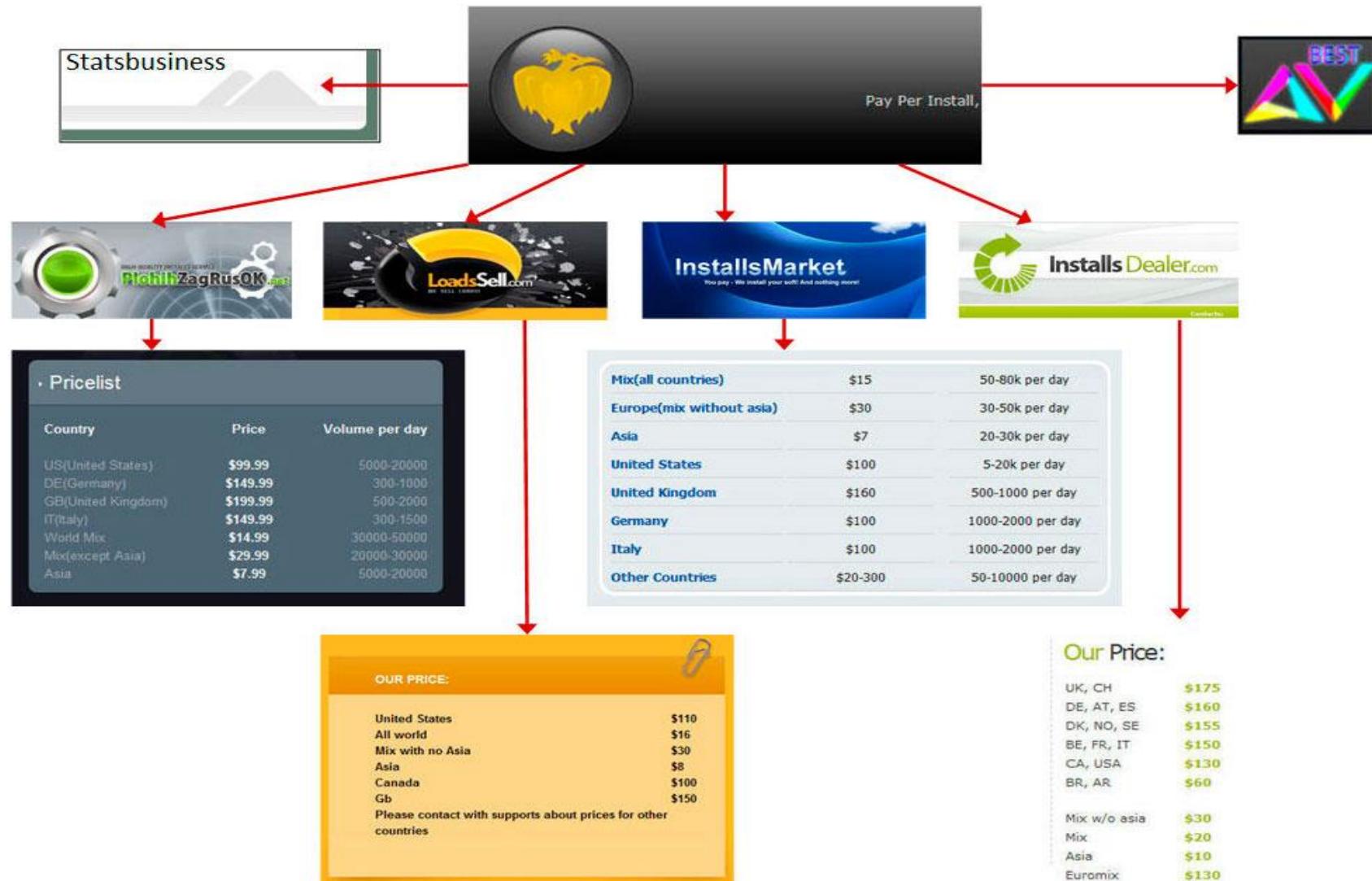
## MARKET PLACE

**Sellers:** Hackers may compromise IT systems and steal data (e.g., NRIC numbers, full name, phone number).

**Buyers:** Scammers may buy this data and try to scam you



# Underground Economy: Example of Pay-per Install Services



# Underground Economy: Size of the Economy?

[CRIME]

## Cyber Crime

**\$97M**

### Fake Antivirus

Users get a message warning them that their computer has been infected with malware. When they click on a link to download antivirus software, their machine is infected. An analysis of financial records from three criminal gangs found that from 2008 to 2010 they collectively earned \$97 million annually.

**\$10M↑**

### Stranded Traveler

Hijacked e-mail accounts are used to ask friends for money, claiming to be stranded traveling abroad. According to an analysis of 2010 records from one e-mail provider, criminals received one or two payments a day, on average.

**\$200M↑**

### Fake Escrow

In a financial transaction, the victim is told to use an "independent" escrow agent. Despite having a convincing website, the escrow company is a sham. There are about 100 active fake escrow websites at any given time, according to a study by the University of Cambridge.

**\$1,000M↑**

### Advanced Fee

Advanced Fee Fraud, sometimes called 419 fraud after the relevant article of the Nigerian criminal code, is legendary for its variations on the same theme. The request is for a small amount (an advance fee) to pay the costs so that a larger fortune can be released.

**\$370M↑**

### Online Banking Fraud: Malware

Cyber thieves target businesses and individuals using malware to capture passwords, account numbers, and other data to get into online banking accounts. As of September 2011, the FBI was investigating 400 cases of "corporate account takeover" where criminals stole \$85 million.

**\$320M=**

### Online Banking Fraud: Phishing

Online banking fraud is sometimes carried out in a phishing attack, in which criminals impersonate websites to get unsuspecting users to provide their login credentials. University of Cambridge researchers estimated that in 2007, between 280,000 and 560,000 people were taken in by fake websites.

Source: Measuring cost of cybercrime  
WEIS 2012

# Underground Economy: Size of the Economy?

[DEFENCE]

## Cyber Defense

**\$1,000M =**

### Bank Countermeasures

Banks sometimes hire companies to vanquish websites used in phishing attacks. There are additional internal security costs, such as authentication programs and systems for generating one-time passwords.

**\$1,000M =**

### Patching Vulnerabilities

Software companies constantly patch their products against vulnerabilities that can be exploited by malware. Anecdotal evidence suggests that the development cost of a single patch for key enterprise software can run up to \$1 million. Deploying that patch is equally costly.

**\$400M**

### Law Enforcement

The authors estimate that the U.S. spends \$200 million to fight cyber crime and accounts for half the law enforcement work worldwide.

**\$3,400M**

### Antivirus

According to a 2010 survey by the European Union's statistics agency, 88 percent of all households with a broadband subscription use some form of antivirus protection.

**\$10,000M =**

### User Cleanup

When antivirus programs fail—or aren't used—users may have to call in the Geek Squad to fix their PC or dump the infected hardware and buy a new machine. The authors calculate the repair cost from malware for U.K. users alone at roughly \$600 million.

**\$40M =**

### ISP Cleanup

In 2010, German Internet Service Providers (ISPs) spent €2 million to establish a call center to help combat botnets—networks of machines that have been infected with malware. In its first year, 315,518 users were notified that they had a compromised machine—a fraction of the infected population.

**\$10,000M =**

### Business Security

Companies use a variety of tools to fight cyber crime including firewalls, intrusion detection systems, software maintenance and deployment, and user training.

Source: Measuring cost of cybercrime  
WEIS 2012

## Underground Economy:

### Size of the Economy? **2019 vs 2012**

crime type	value	changes since 2012	
§3.1 Online credit card fraud	£731.8m (UK)	reduced percentage of turnover	<b>New services -&gt; New Attacks</b>
§3.2 Online bank fraud	£121.4m (UK)	increased, but more activity	
§3.2 Authorised push payments	£236m (UK)	a new category since 2012	
§3.3 In-person card fraud	£158m	has grown but may have peaked	
§3.4 Ransomware	well over \$10m	much increased since 2012	
§3.4 Cryptocrime	\$2bn	was not an issue in 2012	
§3.5 Ad fraud	low \$billions	increased, but no good public data	
§3.5 Pharmaceuticals	tens of \$millions	reduced since 2012	
§3.5 Coupon fraud	\$300m+ (US)	not discussed in 2012	
§3.5 Loyalty-program fraud	\$235m	new since 2012	
§3.5 Travel fraud	\$1bn	new since 2012	
§3.5 Counterfeit software	low \$millions	decreasing trend of 2012 has continued	
§3.5 Copyright theft	low \$10 millions	fallen substantially	<i>Credit card fraud reduced, but phone payments (push payments) increased!</i>
§3.6 Fake antivirus	\$7.1m (US)	down by 90% since 2012	
§3.6 Tech support scams	\$39m (US)	growing very rapidly	
§3.7 Compromised email		regulatory & legal costs now dominate	
§3.8 Fake companies	tens of \$millions	few good figures	
§3.9 Advance fee fraud	low \$100 millions	no reliable estimates	
§3.10 Business email compromise	\$1.3bn (US)	see APP for related UK figure	
§3.11 Telecoms fraud	\$7 billion	markedly down since 2012	
§3.12 WannaCry / NotPetya	\$1–2 billion	one-off events, so may not recur	
§3.13 Fiscal fraud	many \$billions	tax fraud, welfare fraud, etc.	
§3.14 Romance scams	\$143m (US)	more reports than in 2012	

# Data Theft of Personal Records

## Largest Breaches of All Time (records compromised, date reported)



<sup>†</sup> In July data about some 35 million users on Cyworld and Nate (South Korean sites) were swiped, but the types of data are still being verified.

**NEARLY 650 CLIENTS' ACCOUNT INFORMATION STOLEN FROM STANDARD CHARTERED BANK SINGAPORE**

Post date: 5 Dec 2013 - 9:22pm

# Data Theft of Personal Records

## Breach of the Protection Obligation

[businesstimes.com.sg/garage/data-breach-at-reddoorz-hit-6m-customers-hospitality-platform-fined-s74000](https://www.businesstimes.com.sg/garage/data-breach-at-reddoorz-hit-6m-customers-hospitality-platform-fined-s74000)



## Data breach at RedDoorz hit 6m customers; hospitality platform fined S\$74,000

FRI, NOV 12, 2021 - 7:44 AM

CLAUDIA CHONG

4 -min read

Listen to this article



The breach of 5.9 million customer records at RedDoorz was the largest data ...



# Data Theft of Personal Records

## Breach of the Protection Obligation

This included the data of 98,000 Ministry of Defence staff and Singapore Armed Forces servicemen exposed during **a breach in 2019** due to a well-known vulnerability that was knowingly left open for more than four years by healthcare training provider HMI Institute of Health Sciences.

HMI was fined \$35,000 for the incident, according to a judgment issued by the Personal Data Protection Commission (PDPC) last Thursday (June 10).

The incident affected the data of more than 110,000 people in total, including 250 HMI employees.

Web design and e-commerce solutions firm Webcada was fined \$25,000 for a ransomware attack last year affecting the personal data of 520,000 people, who were customers of online shopping websites that the company designed for its clients.



# THE SINGHEALTH BREACH – 1.5 MILLION patient RECORDS STOLEN



# Credit card skimmers target shopping websites popular with Singaporeans, 1,700 cards for sale on Dark Web



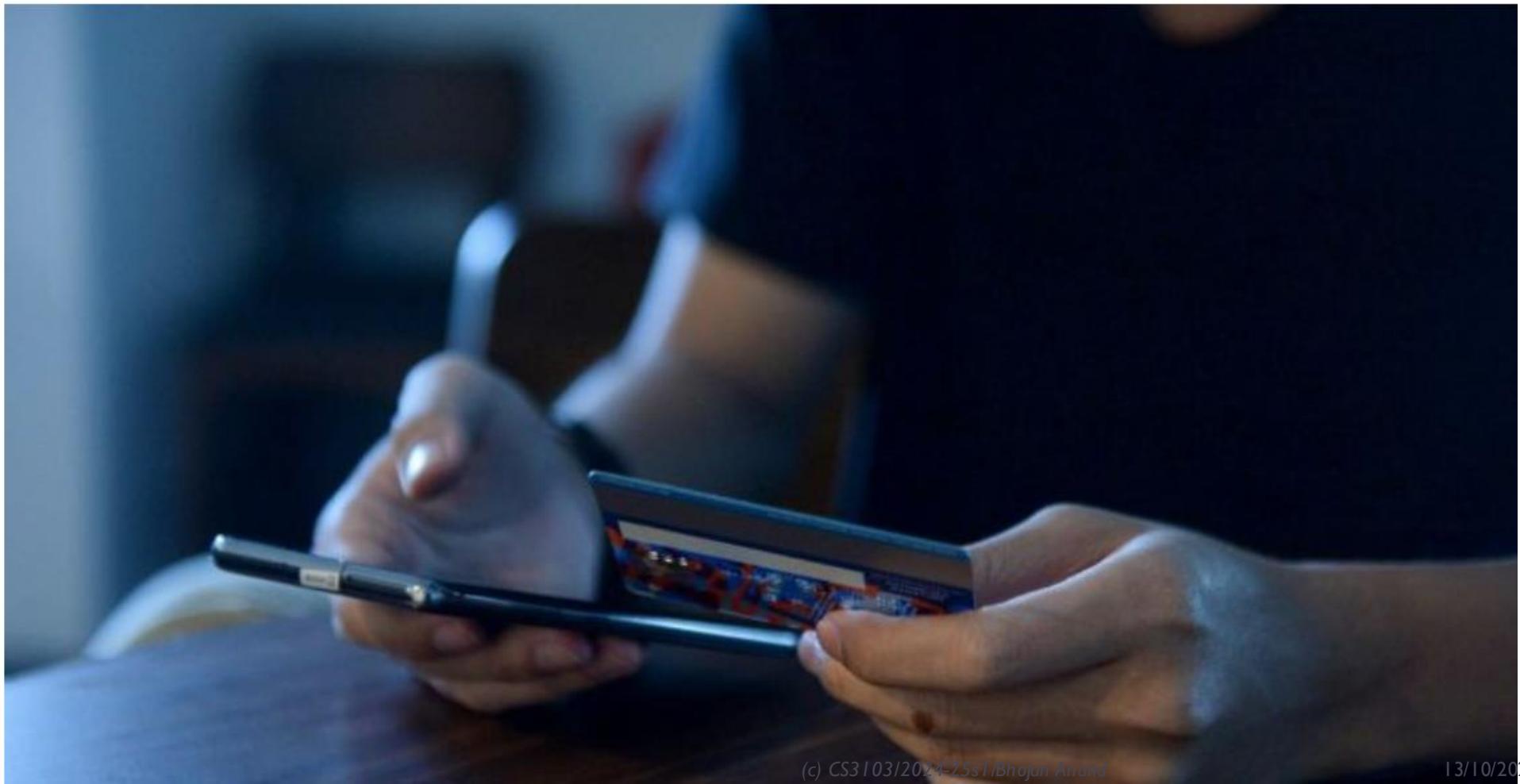
From January to August 2019, the firm had detected 26,102 compromised payment cards issued by Singapore banks that were put up for sale on the Dark Web, with an estimated underground value of US\$1.8 million. ST PHOTO: BHUJAN TAY

(C) CS3103/2024-25s1/Bhojan Anand

13/10/2025

# Credit card data from Singapore on Dark Web priced higher due to rarity: Cyber-security firm

PUBLISHED NOV 29, 2019, 12:00 PM SGT



# OCBC says S\$13.7 million lost in phishing scams, up from S\$8.5 million



People walk past OCBC Bank during lunch break at the Raffles Place financial business district in Singapore on Sep 14, 2021.  
(Photo: AFP/Roslan Rahman)

Source: <https://www.channelnewsasia.com/singapore/ocbc-phishing-scam-more-losses-victims-reported-2469086>

# AI Identity Risk

## AI Ethics Panel: Meanwhile, Bob Logs in as You from 3 Countries at Once.



AI is the #1 creator of new identities with privileged and sensitive access in 2025.

New services -> New Attacks



of respondents lack identity security controls for AI.

#1



cannot secure shadow AI.

Manipulation and access concerns are the primary roadblocks to AI agent adoption.

70%

of respondents say identity silos are a root cause of cybersecurity risk.

49 %

lack complete visibility into entitlements and permissions across their cloud environments.

88 %

are under pressure from insurers mandating enhanced privilege controls.

68 %

say lack of integration between identity and security tools hinders their ability to detect attacks.

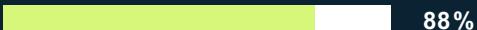
### THE MACHINE IDENTITY EXPLOSION FUELS PRIVILEGE SPRAWL

82:1

Machine identities vastly outnumber humans.

94%

report an increase in machine identities over the past 3 years.



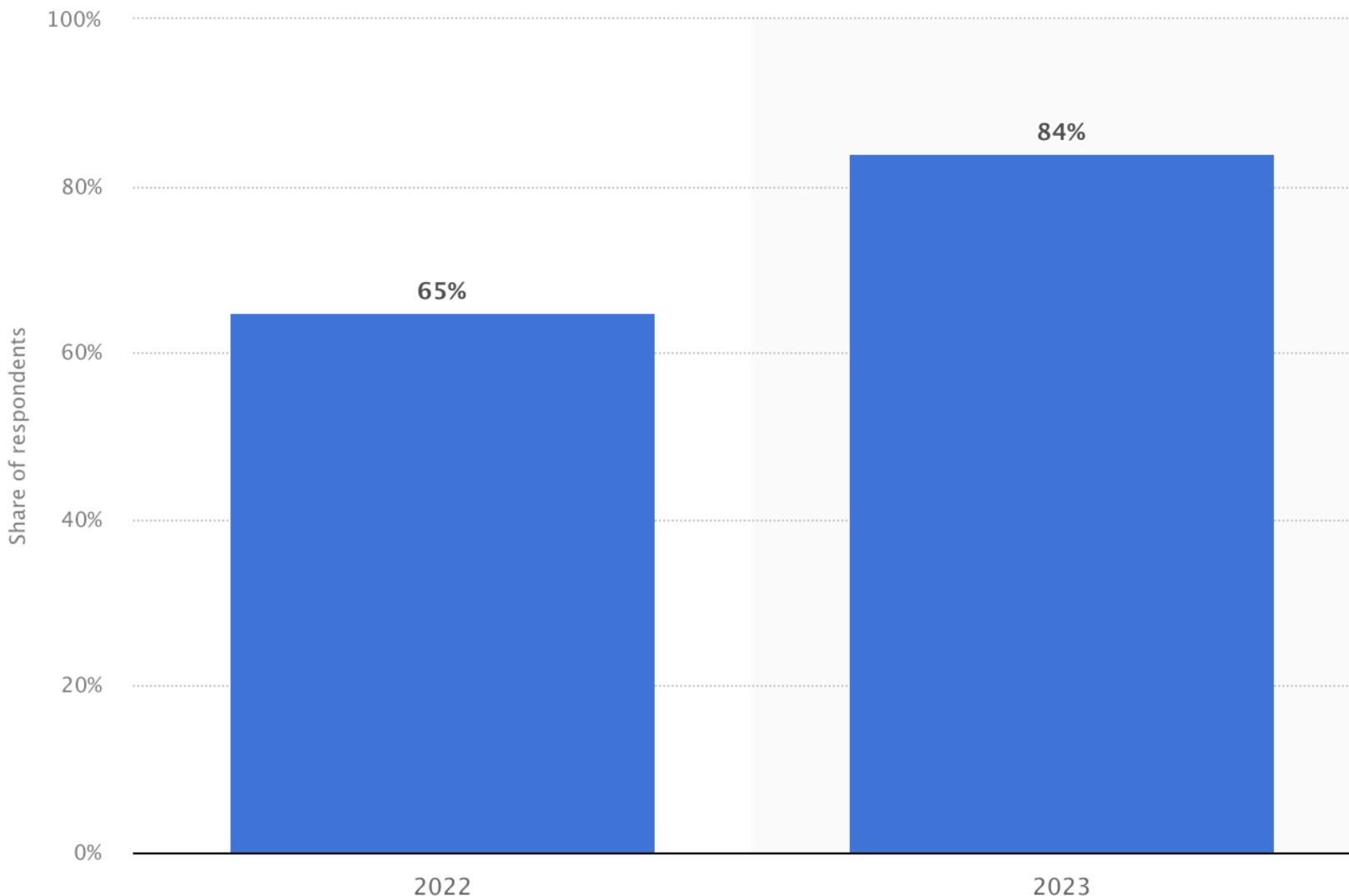
of respondents still define 'privileged users' as human-only.



of machine identities have access to sensitive data.

Source: <https://www.cyberark.com>, 2025 report

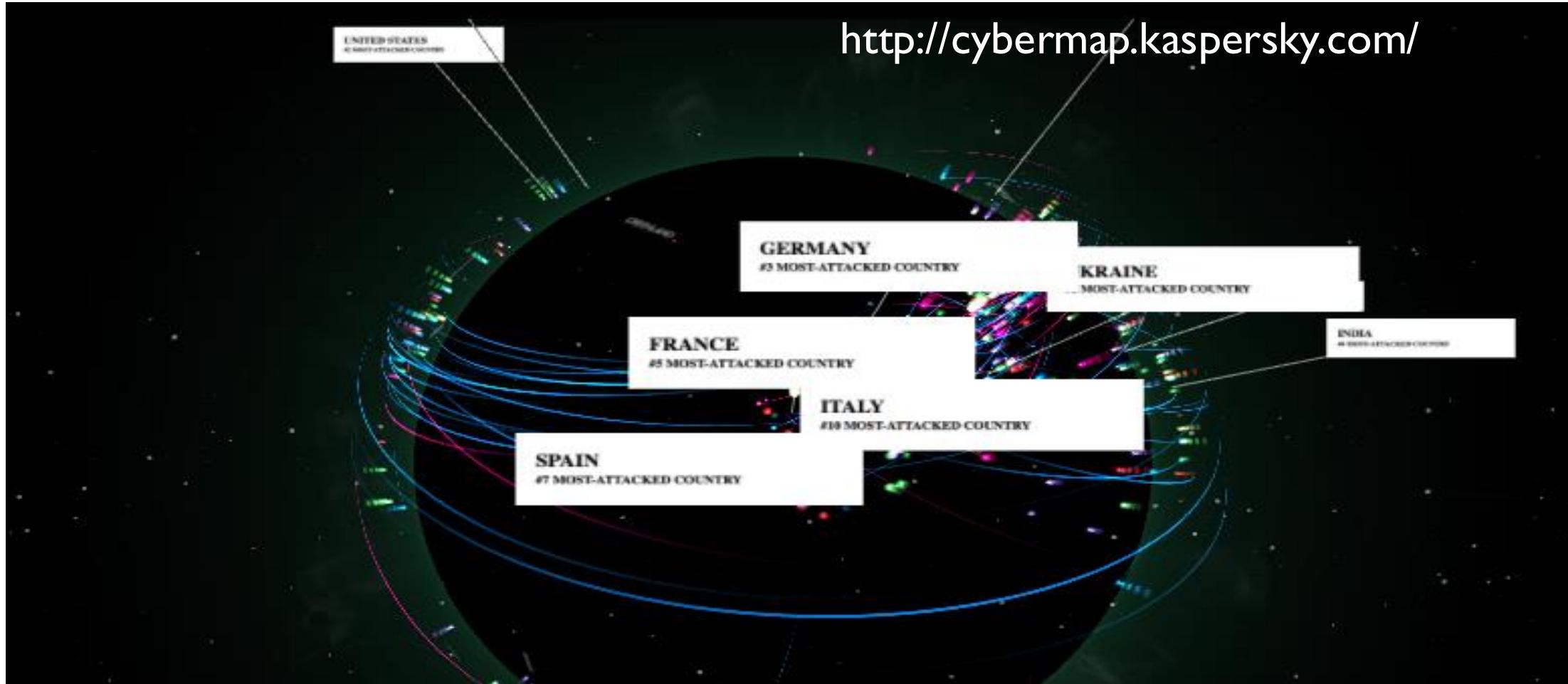
## Share of organizations hit by ransomware attacks in Singapore in 2022 and 2023



In 2023, 84 percent of organizations in Singapore were victims of ransomware attack between **March 2022 and March 2023**, according to a survey conducted among cybersecurity leaders of organizations. **Singapore ranked first worldwide** in terms of ransomware attack rates during this period.

Source: <https://www.statista.com/statistics/1403675/>

# CYBERTHREAT REAL-TIME MAP



All the current cyber attacks occurring around the world in real time. by Kaspersky.com

# Some Experiences

---

- ▶ Credit Card - 2020
- ▶ Stripe payment link - 2022
  
- ▶ Q to research: In 2023, what are the major cyber attacks in Singapore? What are the common vulnerabilities of these systems?



# CS3103: Computer Networks Practice

## Network Security - Intro

### Security Fundamentals

- Attacks on Internet (Self Reading)
- **Services by a Security System (Fast Review)**
- **Security protocols and algorithms (Fast Review)**
  - Internet Security Practices and Examples  
IPsec, TLS, PGP, VPN...

**Dr. Anand Bhojan**

COM3-02-49, School of Computing

[banand@comp.nus.edu.sg](mailto:banand@comp.nus.edu.sg) ph: 651-67351

# Security Services

- 
- 1. Confidentiality
  - 2. Message Integrity
  - 3. Message Authentication
  - 4. Non-repudiation
  - 5. Entity Authentication
  - 6. Access and Availability

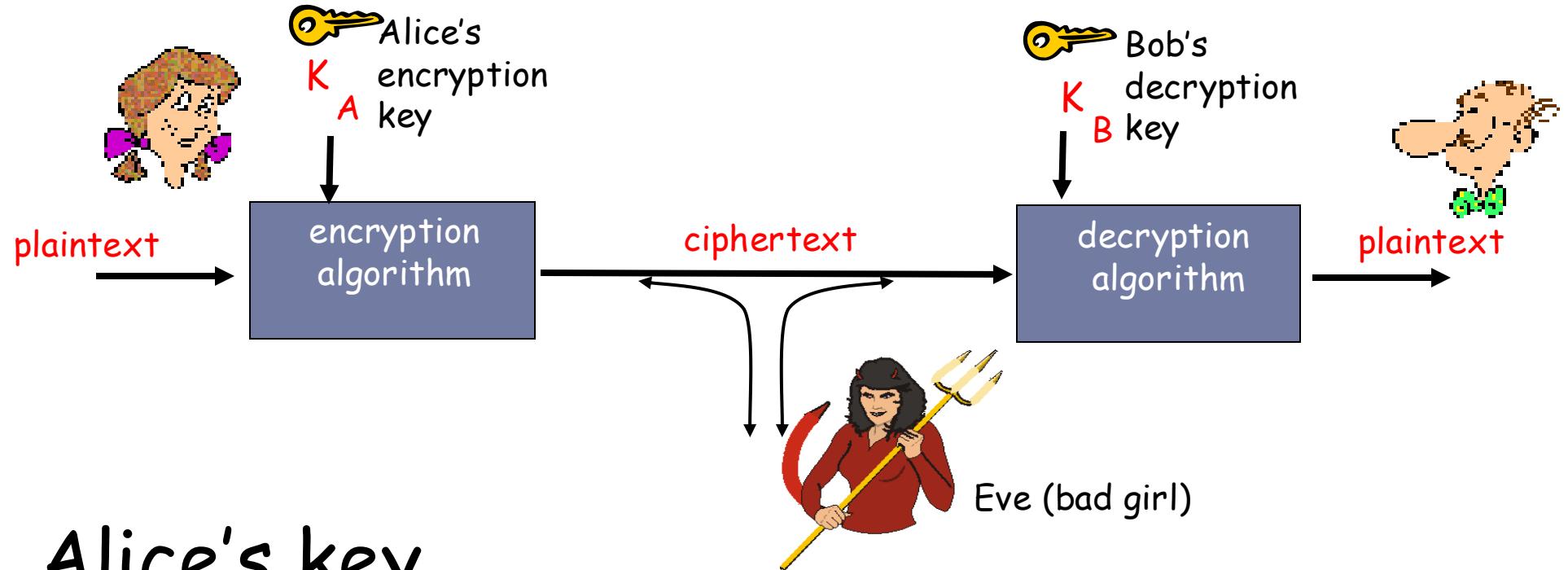
Techniques, Protocols & Algorithms for Security Services ..... (follows)

Heavily Relies on Cryptography

Cryptography heavily relies on Integer Factorisation



# Cryptographic Components

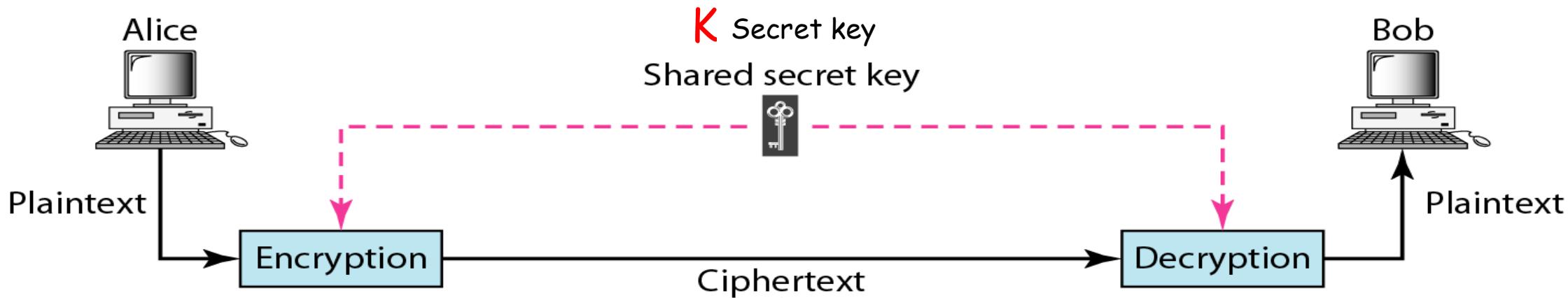


$K_A$  Alice's key  
 $K_B$  Bob's key

Alice, Bob are two entities (person, process, client, server) that like to communicate. Eve is another entity which for eg. intercepts the communication.

# Cryptography- Symmetric key

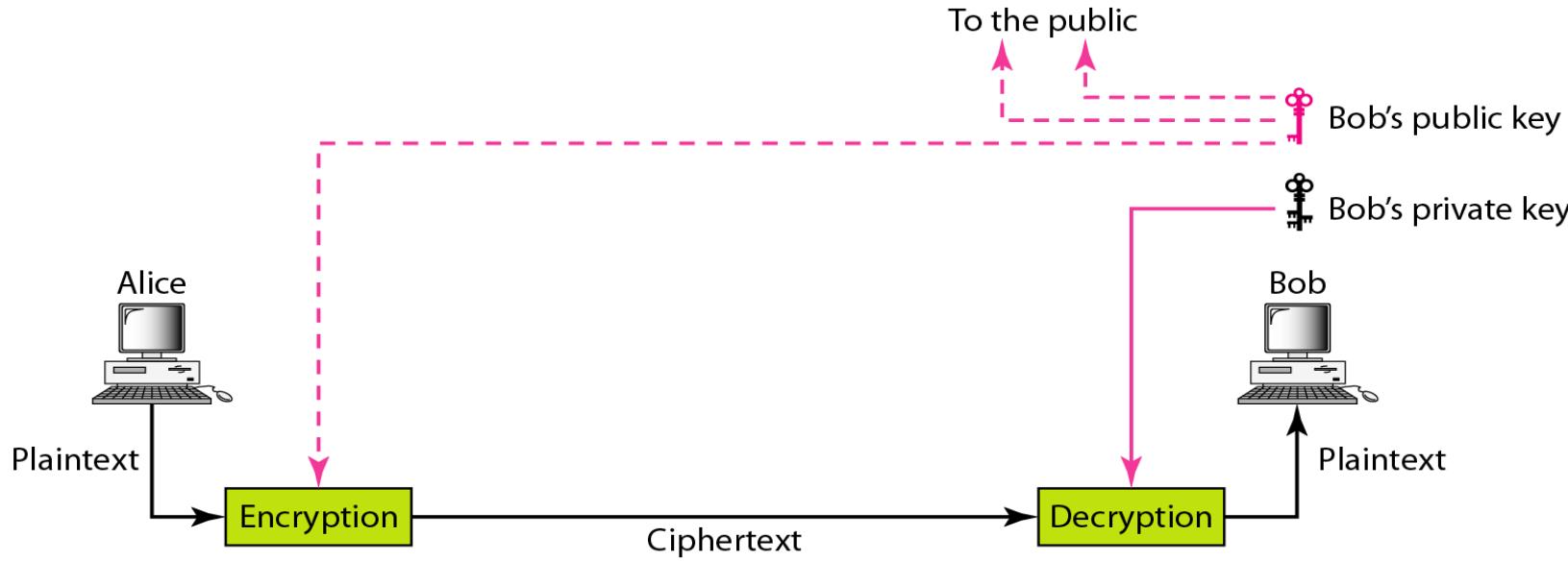
- ▶ symmetric key crypto (*secret-key crypto*): sender, receiver keys *identical*



- ▶ Examples:
  - ▶ Data Encryption Standard (**DES**)
  - ▶ Advanced Encryption Standard (**AES**)

# Cryptography- Asymmetric key

- ▶ public-key crypto (*public-key crypto*): encryption key *public*, decryption key *secret* (*private*)

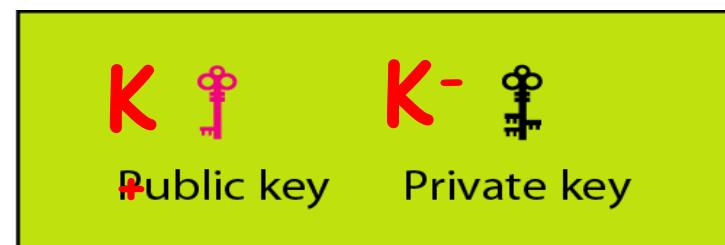


Eg.  
**RSA** (Ron Rivest, Adi Shamir and Leonard Adleman)  
[www.rsa.com](http://www.rsa.com)

**Q: How different keys work together?**



Symmetric-key cryptography



Asymmetric-key cryptography

# Let us test our pre-req knowledge!



<https://pollev.com/banand>

**Caution:-** No random attempts, Some quizzes in this session may be graded for correctness.

Make sure you **LOGIN using your NUSNET ID.**



# Confidentiality

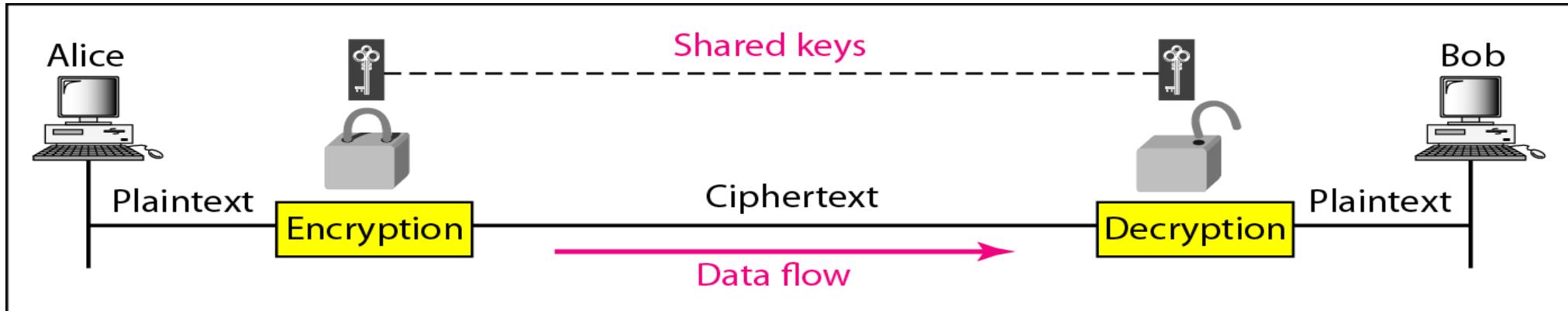
---

only sender, intended receiver should “understand” message contents

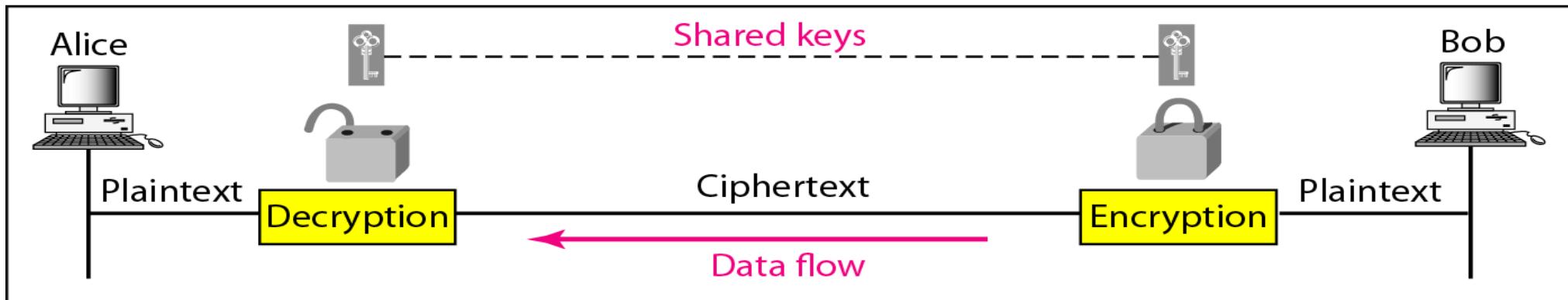
## I. How to send secret messages?



# Confidentiality – **Symmetric key**

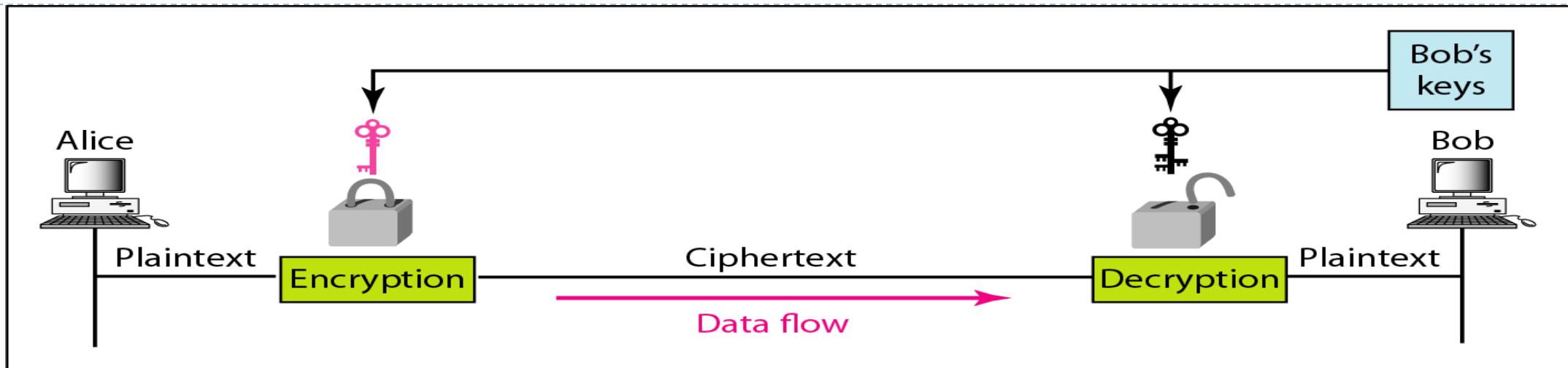


a. A shared secret key can be used in Alice-Bob communication

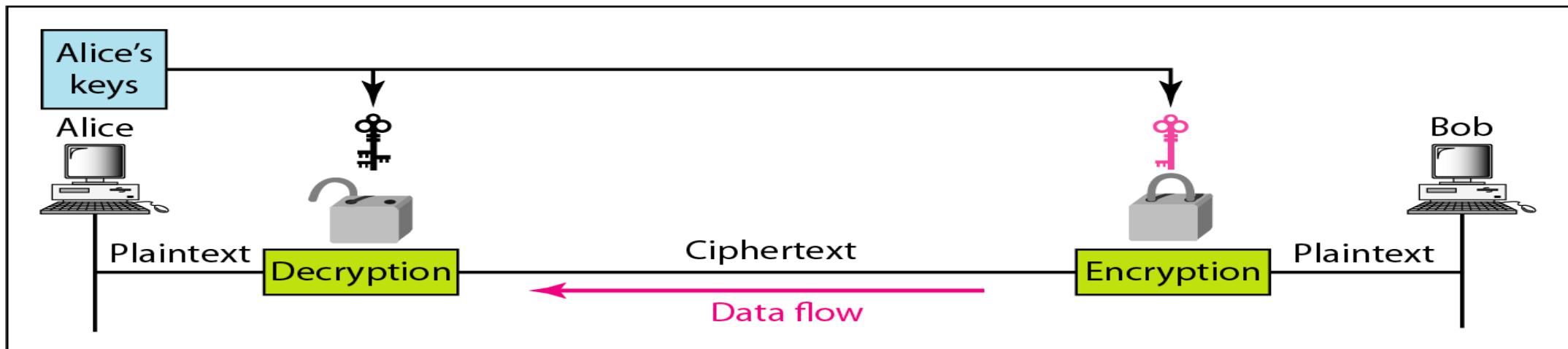


b. A different shared secret key is recommended in Bob-Alice communication

# Confidentiality – **Asymmetric key**



a. Bob's keys are used in Alice-Bob communication



b. Alice's keys are used in Bob-Alice communication

# Message Integrity

---

sender, receiver want to ensure message is **not altered** (in transit, or afterwards) without detection

## 2. How to make sure the message is not altered by Eve?

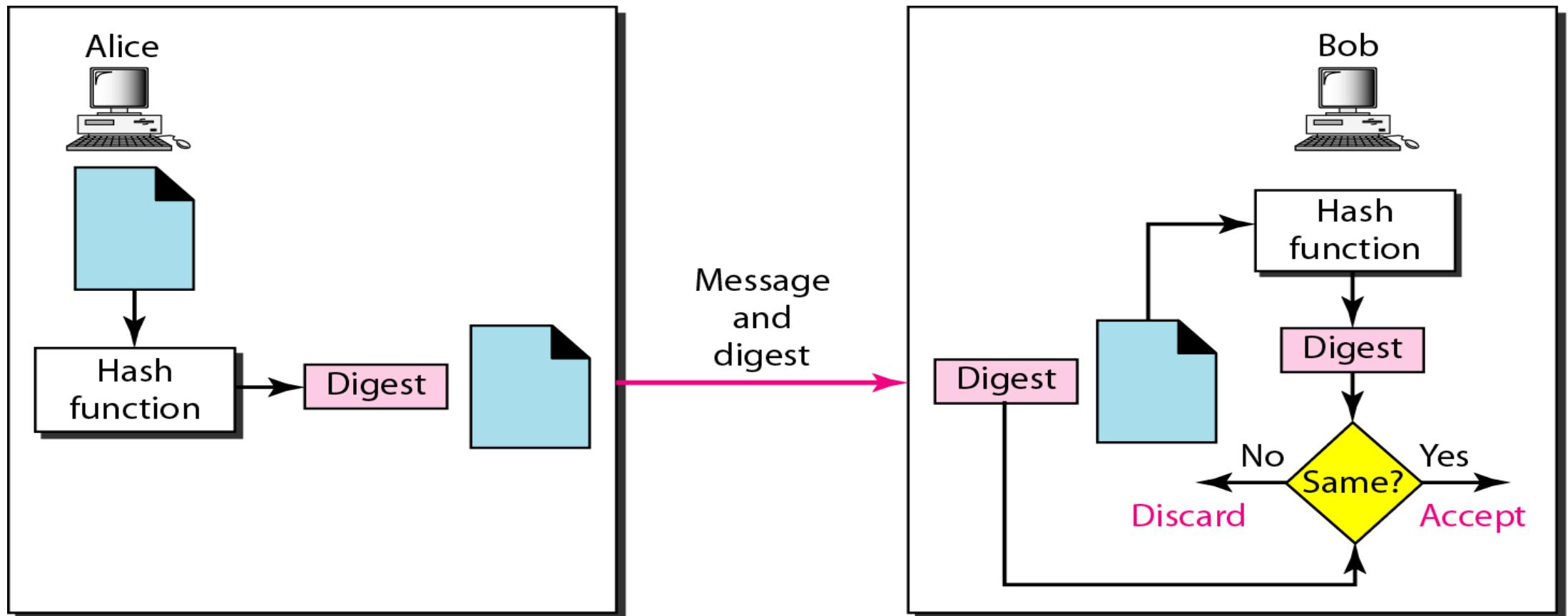


# Message Integrity

- ▶ Message Digest or Modification Detection Code (MDC)
  - ▶ A fixed length “**fingerprint**” of a message  $m$  (of any size) is known as **Message Digest**,  $H(m)$  is generated using a hash function.
  - ▶ **Verifiable** - message is not altered (integrity is ensured).

The Hash function should be a secure hash function that is **one-way**, **collision resistant**, and **pre-image resistant**.

# Message Integrity – Checking



Can It be forged? / Can anyone else ack as Alice?

# Message Authentication

---

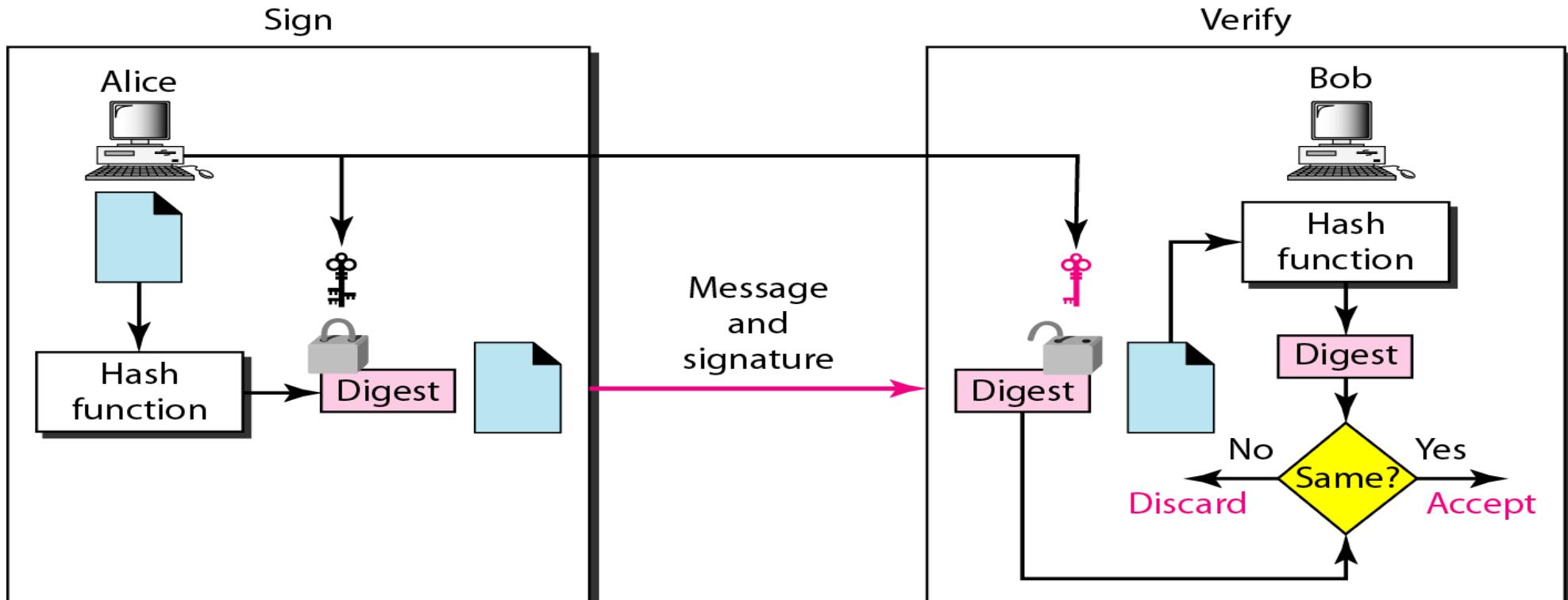
Receiver authenticates the **message** sent by the sender. (may not happen in real-time, eg. e-mail)

## **3. How to make sure the sender is Alice not Eve?**



# Message Authentication - Digital Signatures

- ▶ **Message Authentication Code(MAC)-** symmetric key.
  - ▶  $H(\text{Message} + \text{Key})$
- ▶ **Digital Signature (signing a message)**
  - ▶ Uses asymmetric key
  - ▶ **Verifiable, non-forgable and provides authentication.**



# Non-repudiation

---

Sender must not be able to deny sending a message that he did send.

**4a. What if the sender deny sending a message that he/she did send?**

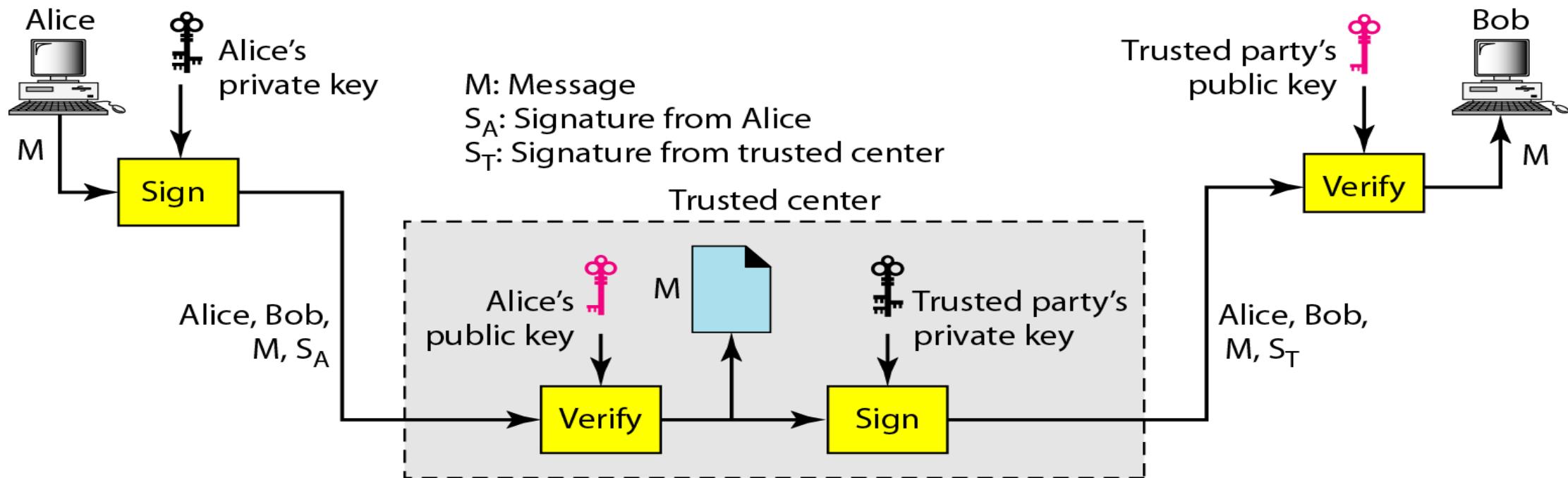
**4b.What if the sender claims the signature is not authentic?**

**4c.What if the sender changes his/her public key?**

**With trusted center (third party)!**

# Digital Signature - Non-repudiation

- ▶ Non-repudiation using trusted third party



# Entity Authentication (User Authentication)

---

Bank needs to authenticate the user before any message communication starts. (real-time, one time authentication for series of messages, online-banking)

Is this person or system really who they say they are, right now?

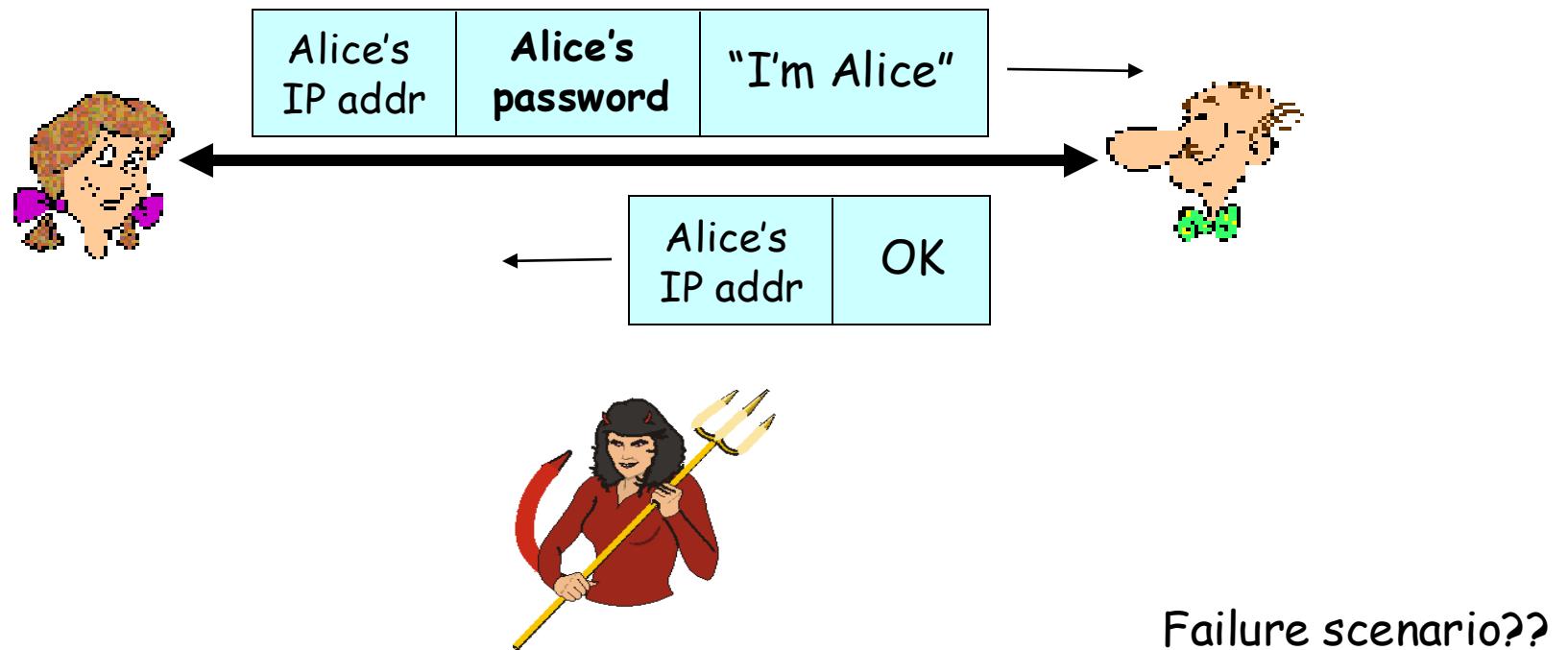
**5.What if the user wants to send and receive a series of secured messages in real-time? Do we need to authenticate each message separately?**

User authentication can also be done using Private key!



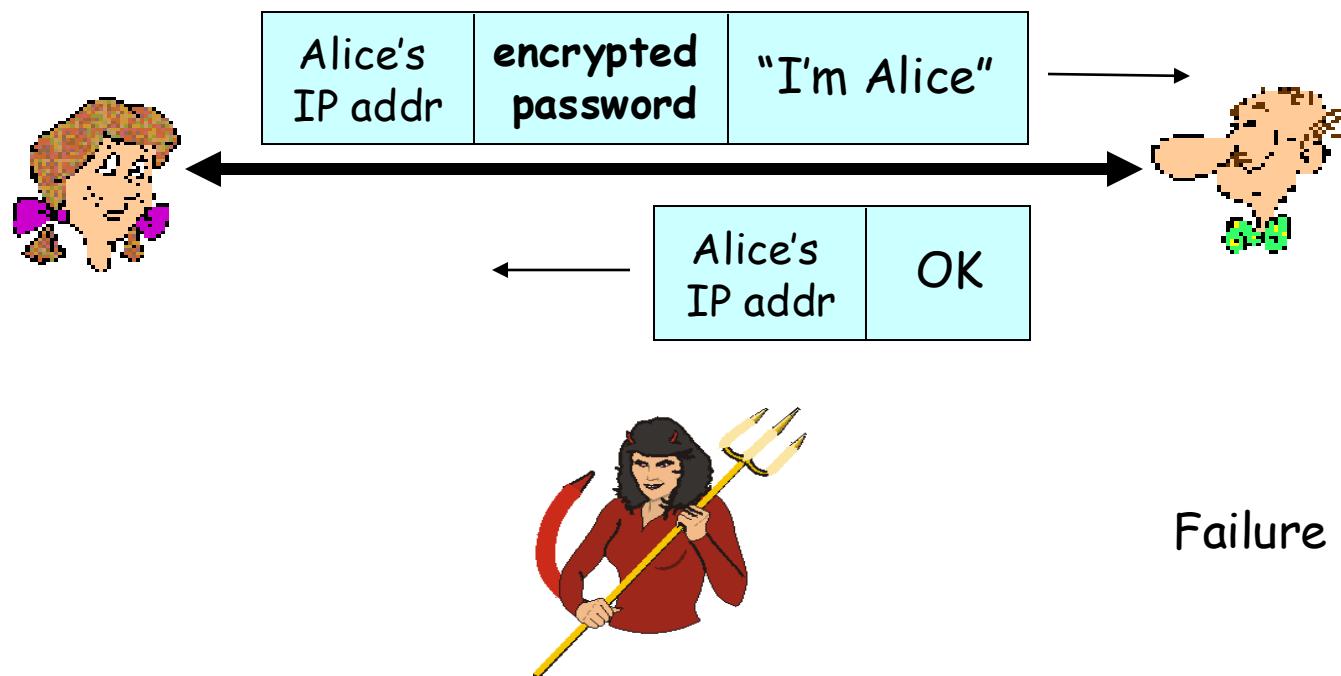
# Entity Authentication

- ▶ Protocol apI.0: Alice says “I am Alice” and sends her secret password to “prove” it.



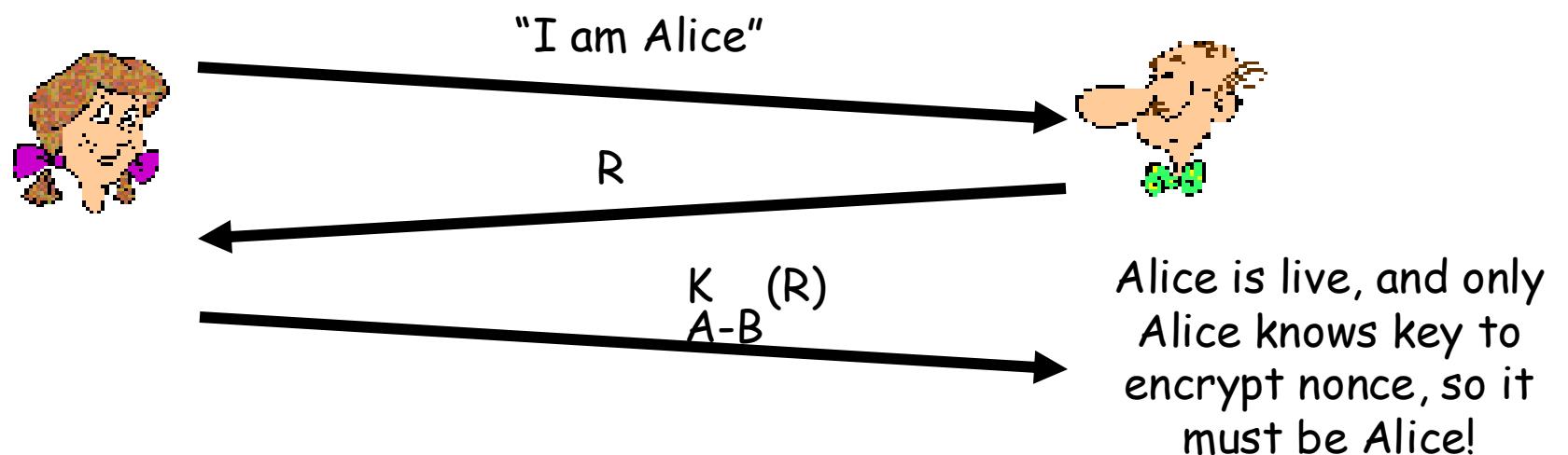
# Entity Authentication

- ▶ Protocol apI.I: Alice says “I am Alice” and sends her *encrypted* secret password to “prove” it.



# Entity Authentication (Challenge-Response with **symmetric key**)

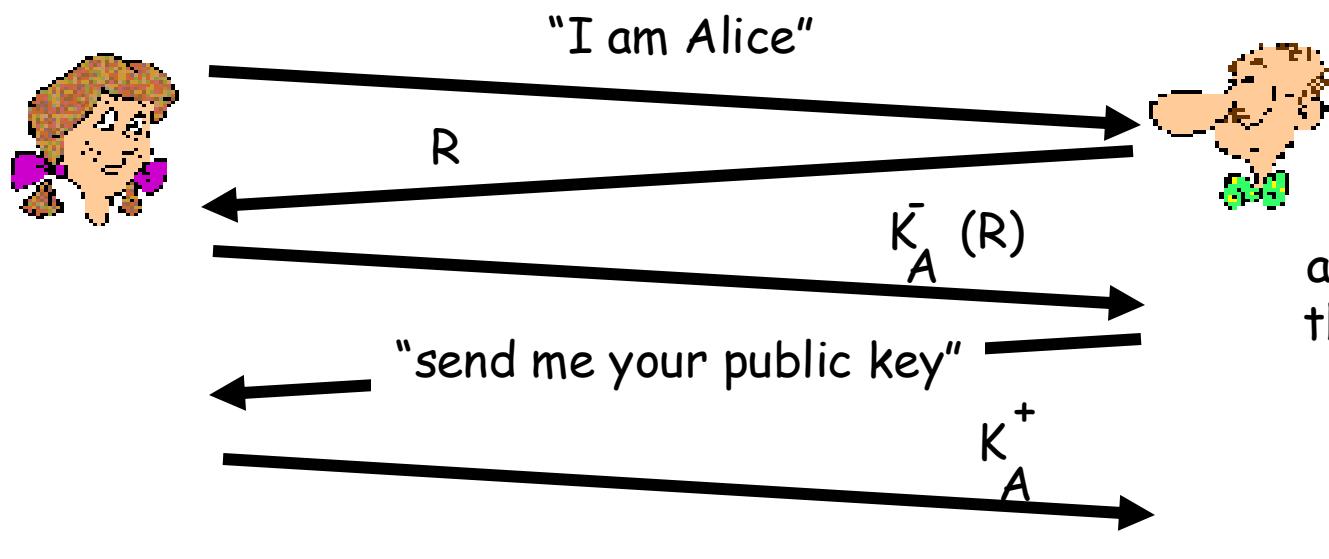
- ▶ Nonce/challenge: number ( $R$ ) used only *once-in-a-lifetime*
- ▶ ap4.0: to prove Alice “live”, Bob sends Alice **nonce**,  $R$ . Alice must return  $R$ , encrypted with **shared secret key**



Can use ‘time stamp’ instead of nonce, if Alice and Bob are time synchronized.

# Entity Authentication (Challenge-Response with **asymmetric key**)

- ▶ ap5.0: uses nonce, public key cryptography
  - ▶ ap4.0 requires shared symmetric key
  - can we authenticate using public key techniques?



$\bar{K}_A$  A's private key

$K_A^+$  A's public key

Bob computes  
 $K_A^+(\bar{K}_A(R)) = R$   
and knows only Alice could have  
the private key, that encrypted  
 $R$  such that

$$K_A^+(\bar{K}_A(R)) = R$$

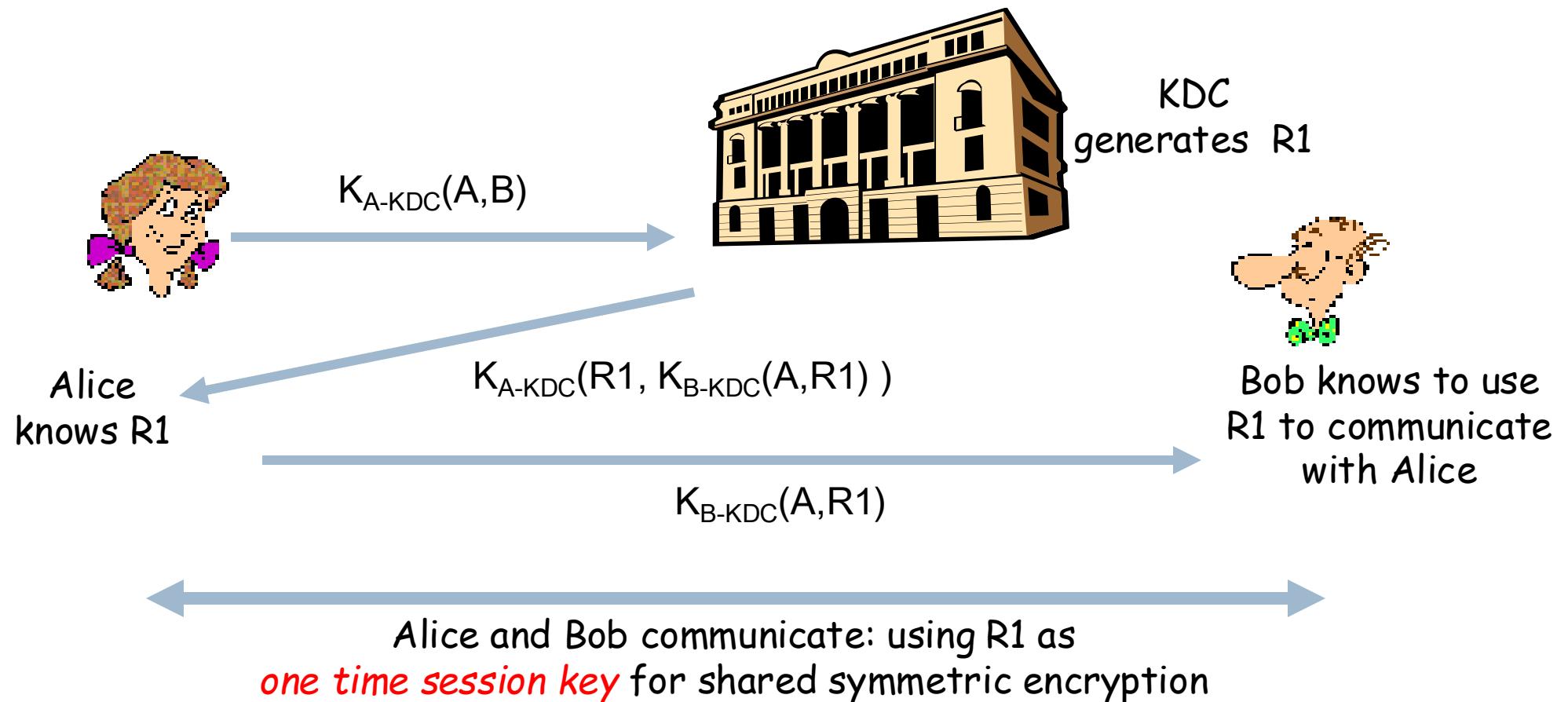
Q: Find the security hole in ap5.0?  
Q: How to solve?

# Key distribution and Certification

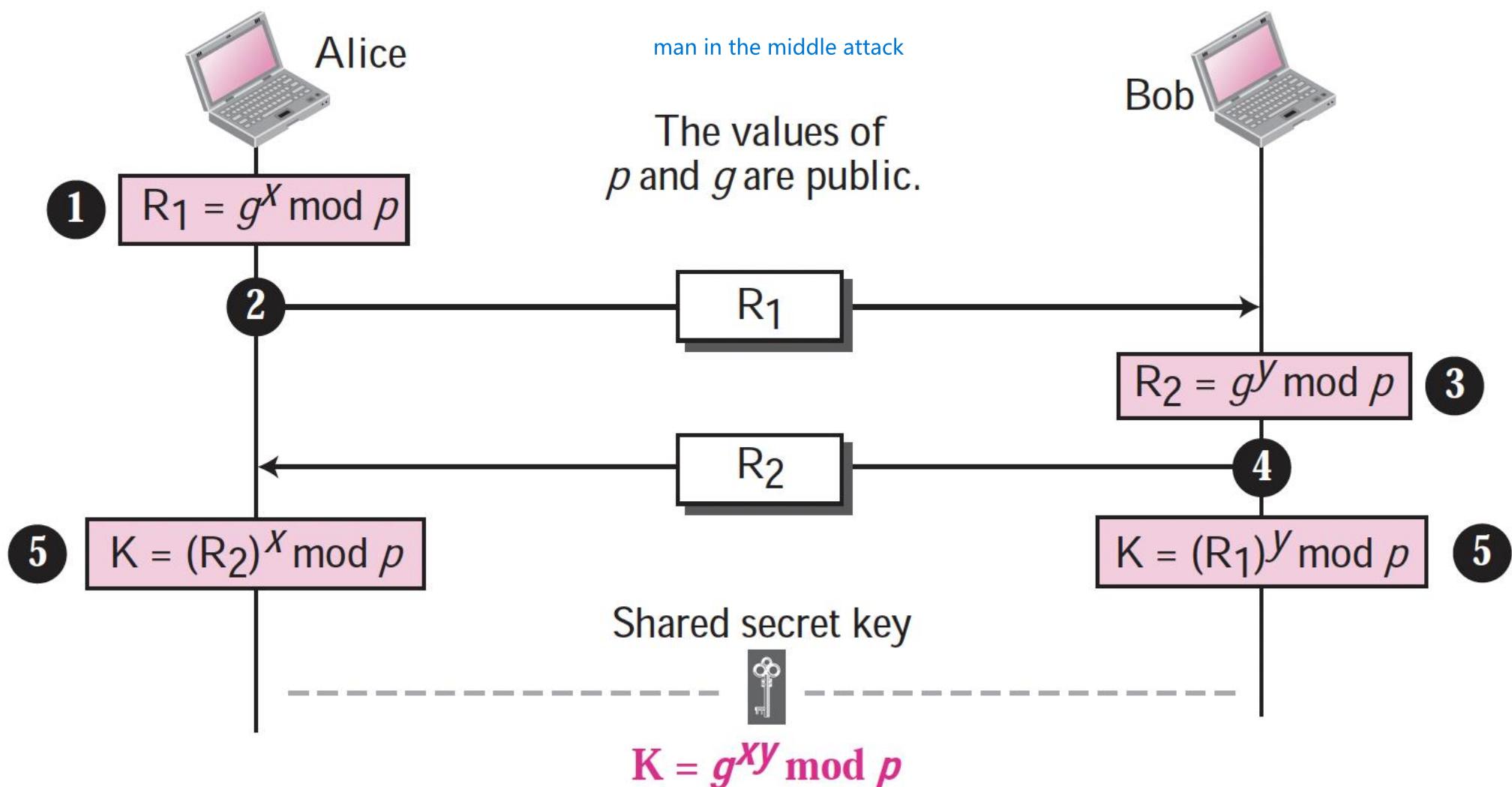
- ▶ Symmetric key Cryptography
  - ▶ Distribution of secret key?
  - ▶ **KDC**- Key Distribution Center
    - ▶ Each party should have a symmetric secret key to the KDC.
    - ▶ Easy to revoke
  - ▶ **Q:What is Kerberos?**
- ▶ Public Key Cryptography
  - ▶ Obtaining someone's true public key?
  - ▶ **CA** – Certification Authority
    - ▶ Certifies a public key belongs to a particular entity
    - ▶ Once a public key is certified, then it can be distributed from anywhere, including a public key server, personal Web page or a diskette.
    - ▶ Hard to revoke.

# Key Distribution Center (KDC)

**Q:** How does KDC allow Bob, Alice to determine shared symmetric secret key to communicate with each other?



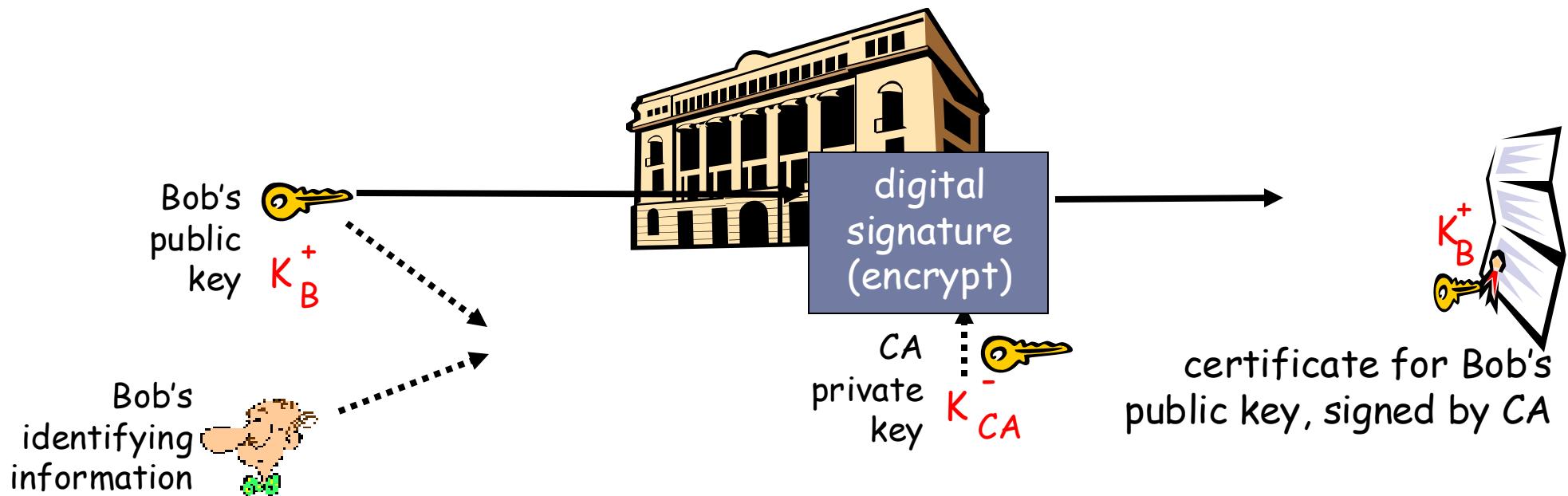
# Diffie Hellman – Key Exchange Protocol [without KDC]



**Ephemeral Diffie-Hellman** : Changes all keys  $p, q, x, y$  each time the algorithm is run.

# Certification Authorities

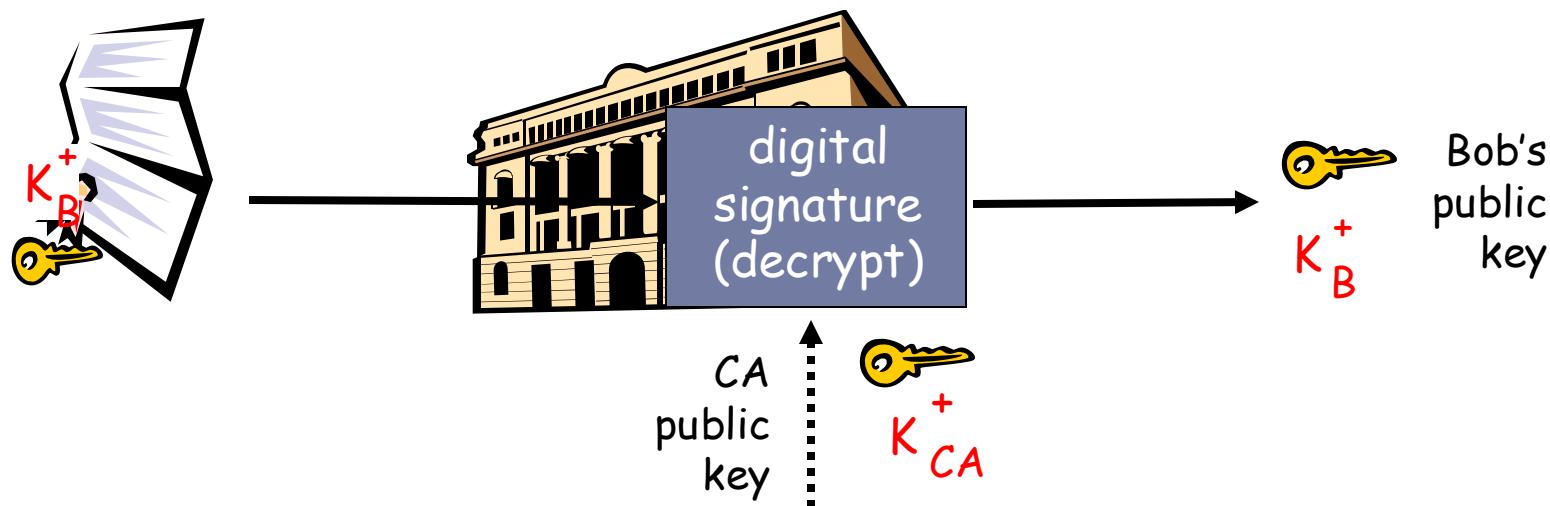
- ▶ **Certification authority (CA):** binds public key to particular entity, E.
- ▶ E (person, router) registers its public key with CA.
  - ▶ E provides “proof of identity” to CA.
  - ▶ CA creates certificate binding E to its public key.
  - ▶ certificate containing E's public key digitally signed by CA – CA says “this is E's public key”



# Certification Authorities

When Alice wants Bob's public key:

- gets Bob's certificate (Bob or elsewhere).
- apply CA's public key to Bob's certificate, get Bob's public key



# Certificate Authorities

- ▶ CA has solved the problem of public-key fraud, it has created a side effect. Each certificate may have different format. Hard to automate sw to download certificates and extract the public key.
- ▶ Standards:
  - ▶ ITU and IETF
  - ▶ ITU X.509 [ITU 1993]
    - ▶ Authentication service
    - ▶ Syntax for certificates
    - ▶ RFC 1422 – CA based key management for use with secure internet e-mail.

# A certificate contains:

canvas.nus.edu.sg

Certificate Viewer: canvas.nus.edu.sg

**General** Details

**Issued To**

Common Name (CN)	canvas.nus.edu.sg
Organisation (O)	<Not part of certificate>
Organisational Unit (OU)	<Not part of certificate>

**Issued By**

Common Name (CN)	R11
Organisation (O)	Let's Encrypt
Organisational Unit (OU)	<Not part of certificate>

**Validity Period**

Issued On	Thursday 12 September 2024 at 08:55:33
Expires On	Wednesday 11 December 2024 at 08:55:32

**SHA-256 Fingerprints**

Certificate	134f28957c32ef87f49d092b6b7b59adcfaa1302746ca6de2e42ed5548aef72b
Public key	cac51942c73cf1f0112320d57d8a234387064ef5eaacdac2fe3e0842f23cf01e

uvents.nus.edu.sg/homepage/events

Certificate Viewer: \*.nus.edu.sg

**General** Details

**Issued To**

Common Name (CN)	*.nus.edu.sg
Organisation (O)	National University of Singapore
Organisational Unit (OU)	<Not part of certificate>

**Issued By**

Common Name (CN)	Entrust Certification Authority - L1K
Organisation (O)	Entrust, Inc.
Organisational Unit (OU)	See <a href="http://www.entrust.net/legal-terms">www.entrust.net/legal-terms</a>

**Validity Period**

Issued On	Friday 27 September 2024 at 14:56:17
Expires On	Saturday 27 September 2025 at 14:56:16

**SHA-256 Fingerprints**

Certificate	9f28011b368dc0634d4f822eef507b080551bae3a11424cf341e576791a01110
Public key	b7c14f5ac72046d371396d3114f9c91989a419ec2194bdf9b2084315136b27d4

# Assess and Availability

---

Services must be accessible and available to users.

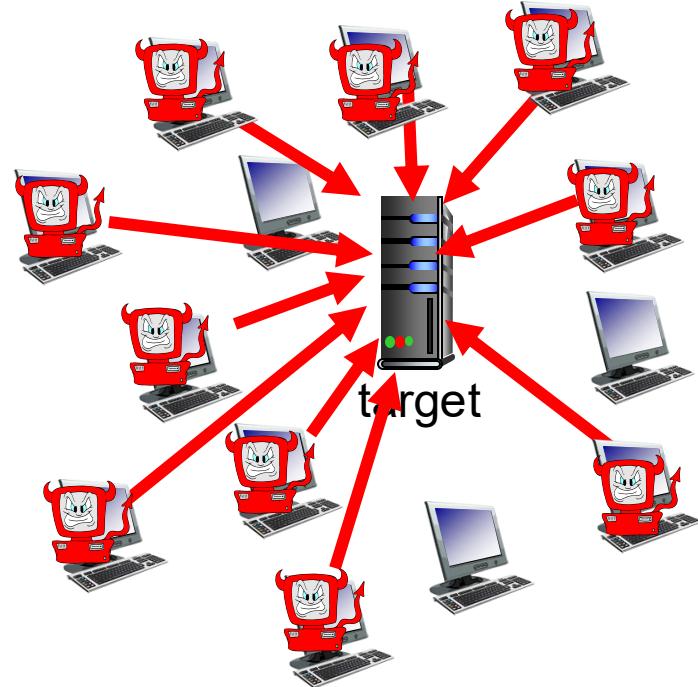
**6. Eve can make the service not accessible or unavailable to Alice. How to defend such attacks?**



# Bad guys: denial of service

*Distributed Denial of Service (DDoS):* attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

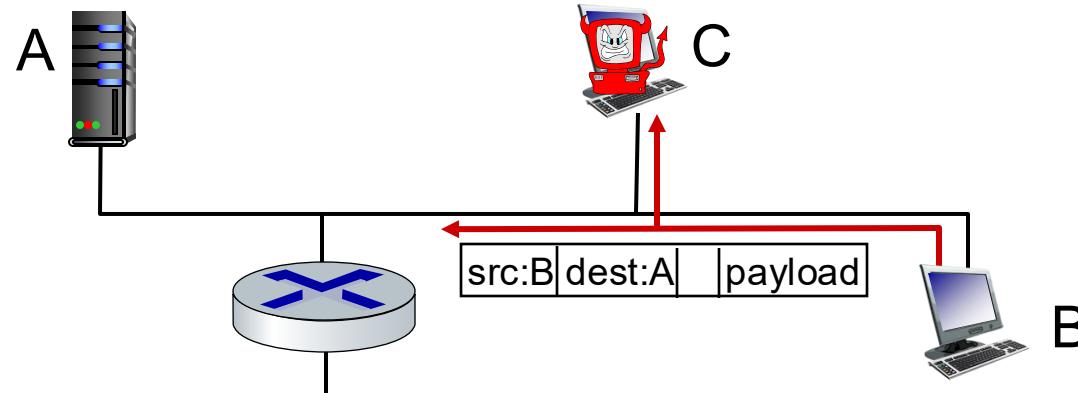
1. select target
2. break into hosts  
around the network  
(see **botnet**)
3. send packets to target  
from compromised  
hosts



# Bad Guys: packet interception

## *packet “sniffing”:*

- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



Wireshark software packet-sniffer

# Access and Availability

---

- ▶ Countermeasures?
- ▶ Denial of Service
  - ▶ **filter out flooded packets (e.g., SYN) before reaching host: throw out good with bad! (Firewall)**
  - ▶ **traceback** to source of floods (most likely an innocent, compromised machine)

# Break...



Source: <http://www.grantland.net/infosecurity2.htm>

# CS3103: Computer Networks Practice

## Network Security

### Security Fundamentals

- Attacks on Internet (Self Reading)
- Services by a Security System (Fast Review)
- Security protocols and algorithms (Fast Review)
- **Internet Security Practices and Examples  
IPsec, TLS, PGP, VPN...**

**Dr. Anand Bhojan**

COM3-02-49, School of Computing

[banand@comp.nus.edu.sg](mailto:banand@comp.nus.edu.sg) ph: 651-67351

# Internet Security Practices

---

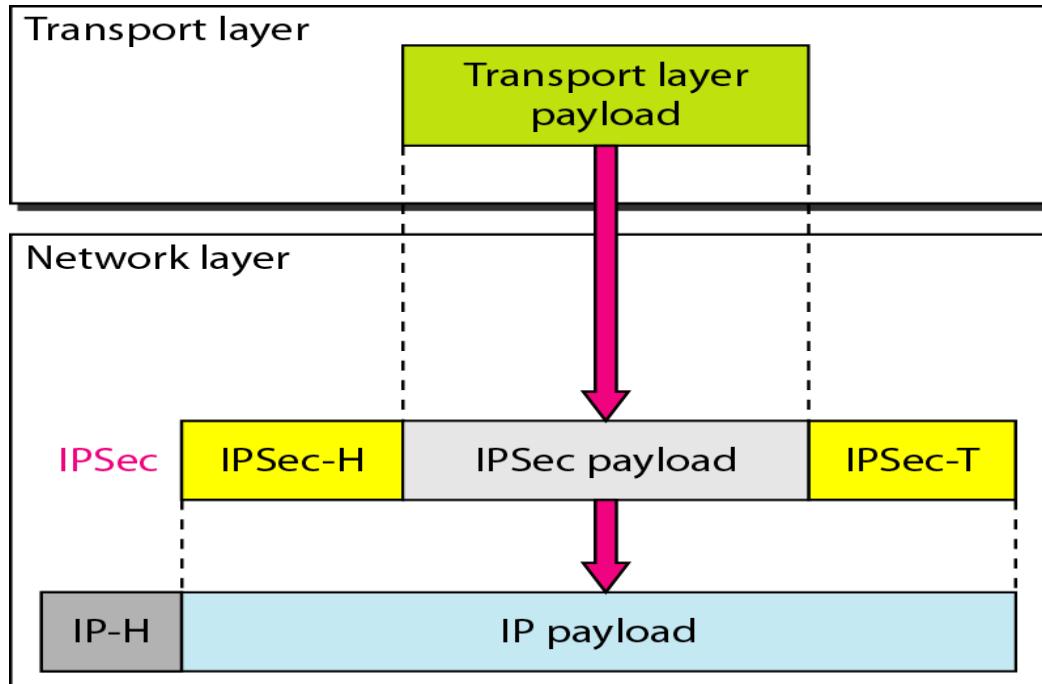
- ▶ Choice of Implementing Security Services
- ▶ Application Layer
- ▶ Transport Layer
- ▶ Network layer

# Network Layer Security – IPsec

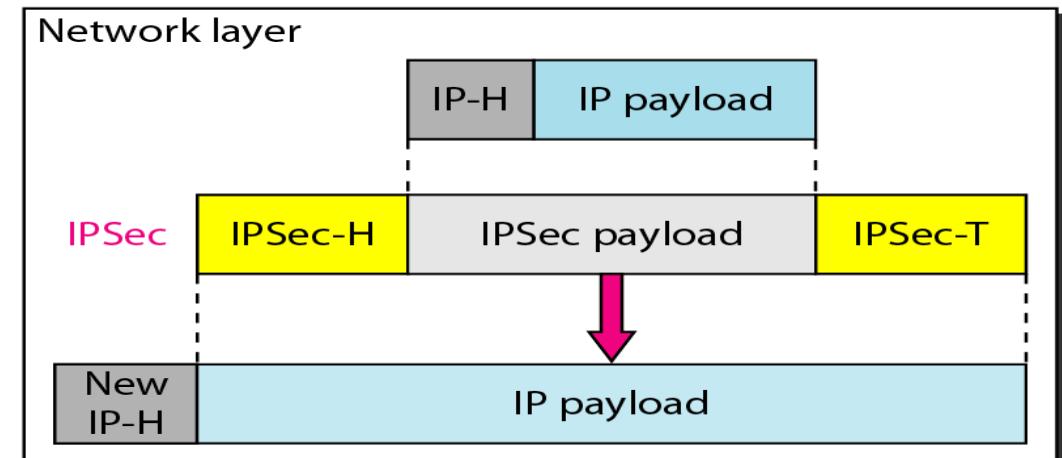
- **Network-layer secrecy:**
  - \* sending host encrypts the data in IP datagram:
    - \* TCP and UDP segments
    - \* ICMP and SNMP messages
- **Network-layer authentication**
  - \* destination host can authenticate source IP address

**Q: Pros and Cons of network layer security?**

# IPsec Modes



a. Transport mode

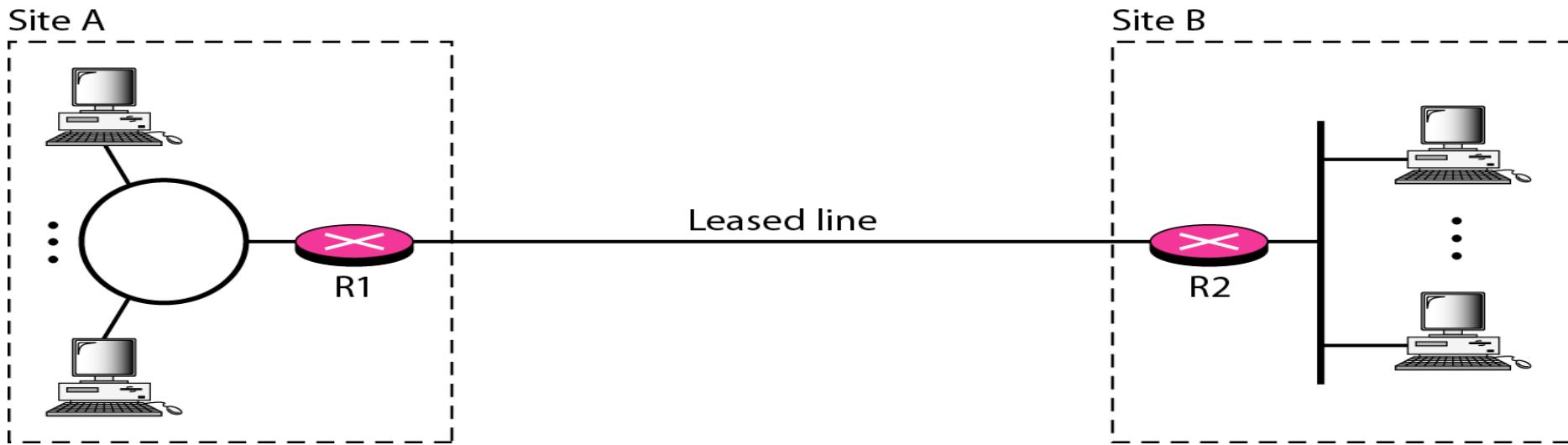


b. Tunnel mode

- IPsec in the **transport mode** does not protect the IP header; it only protects the information coming from the transport layer.
- IPsec in **tunnel mode** protects the original IP header.

# IPsec in Use -- VPN (Virtual Private Networks)

## **Private Internet** - Internet of Private LANs and Private WANs

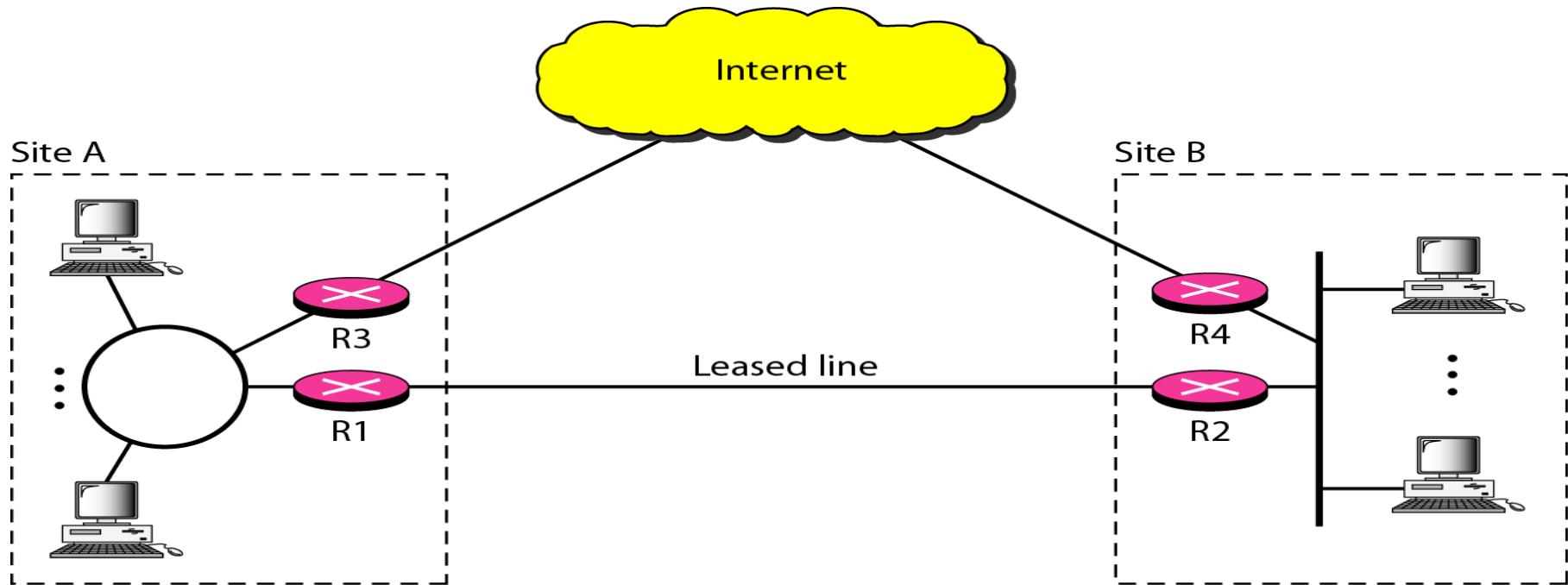


Private  
Addresses

	<i>Prefix</i>	<i>Range</i>	<i>Total</i>
	10/8	10.0.0.0 to 10.255.255.255	$2^{24}$
	172.16/12	172.16.0.0 to 172.31.255.255	$2^{20}$
	192.168/16	192.168.0.0 to 192.168.255.255	$2^{16}$

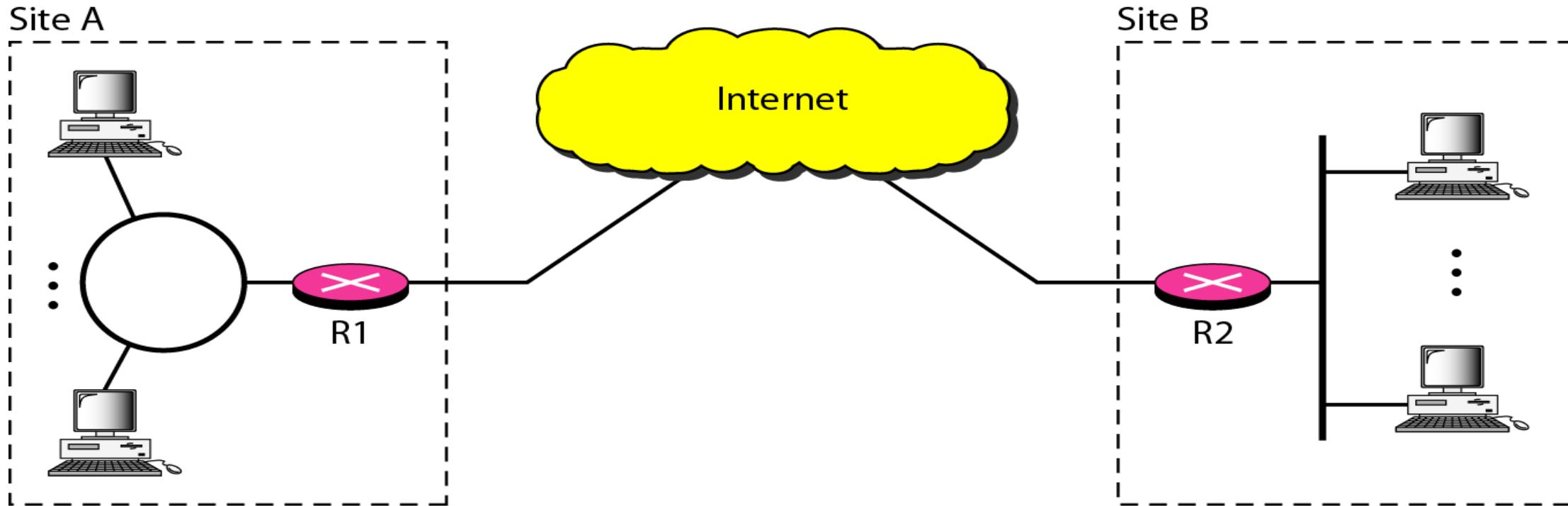
# IPsec in Use -- VPN (Virtual Private Networks)

## Hybrid Network – private internet and public internet



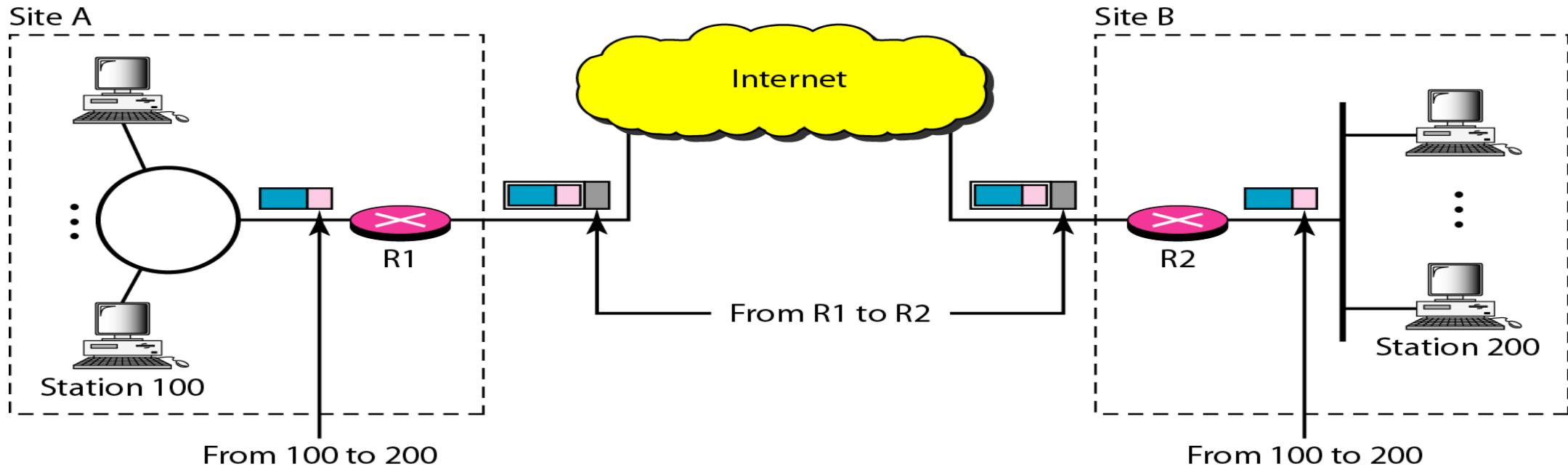
# IPsec in Use -- VPN (Virtual Private Networks)

**Virtual Private Network** - Private internet using the public internet



# IPsec in Use -- VPN (Virtual Private Networks)

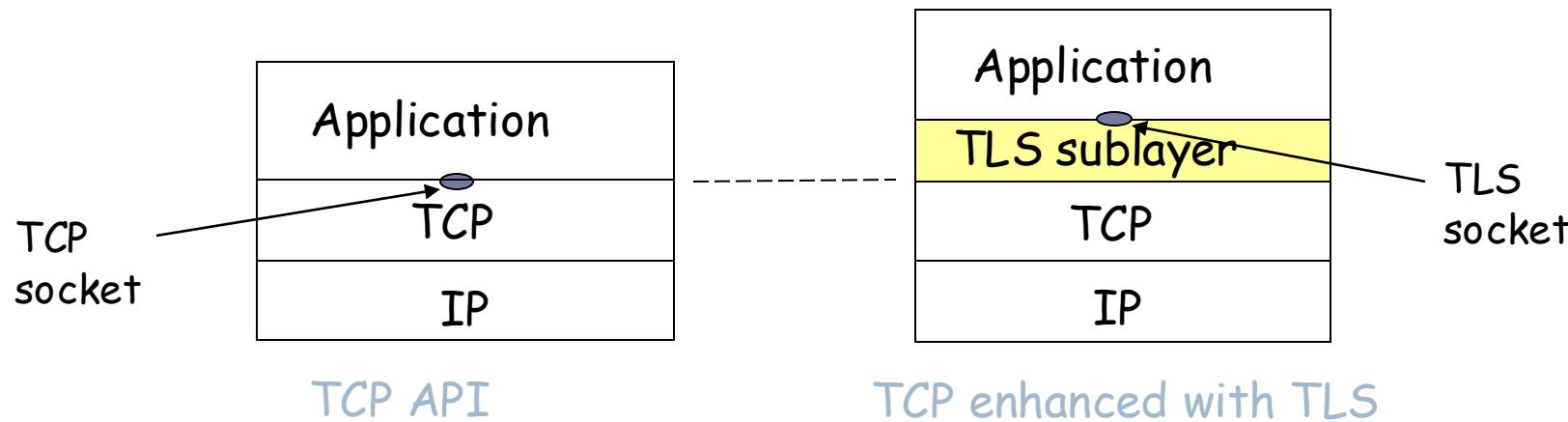
## Virtual Private Network – Addressing



VPN technology uses **IPsec** in **tunnel mode** to provide authentication, integrity, and privacy

# Transport Layer Security (TLS) - Securing the Web apps

- transport layer security to any TCP-based app using TLS services.
- used between Web browsers, servers for e-commerce (https).
- security services:
  - confidentiality:** via symmetric encryption
  - integrity:** via cryptographic hashing
  - authentication:** via public key cryptography
- Bit History: **secure socket layer (SSL)** deprecated [2015]; **TLS 1.3:** RFC 8846 [2018]



# A toy-TLS Handshake

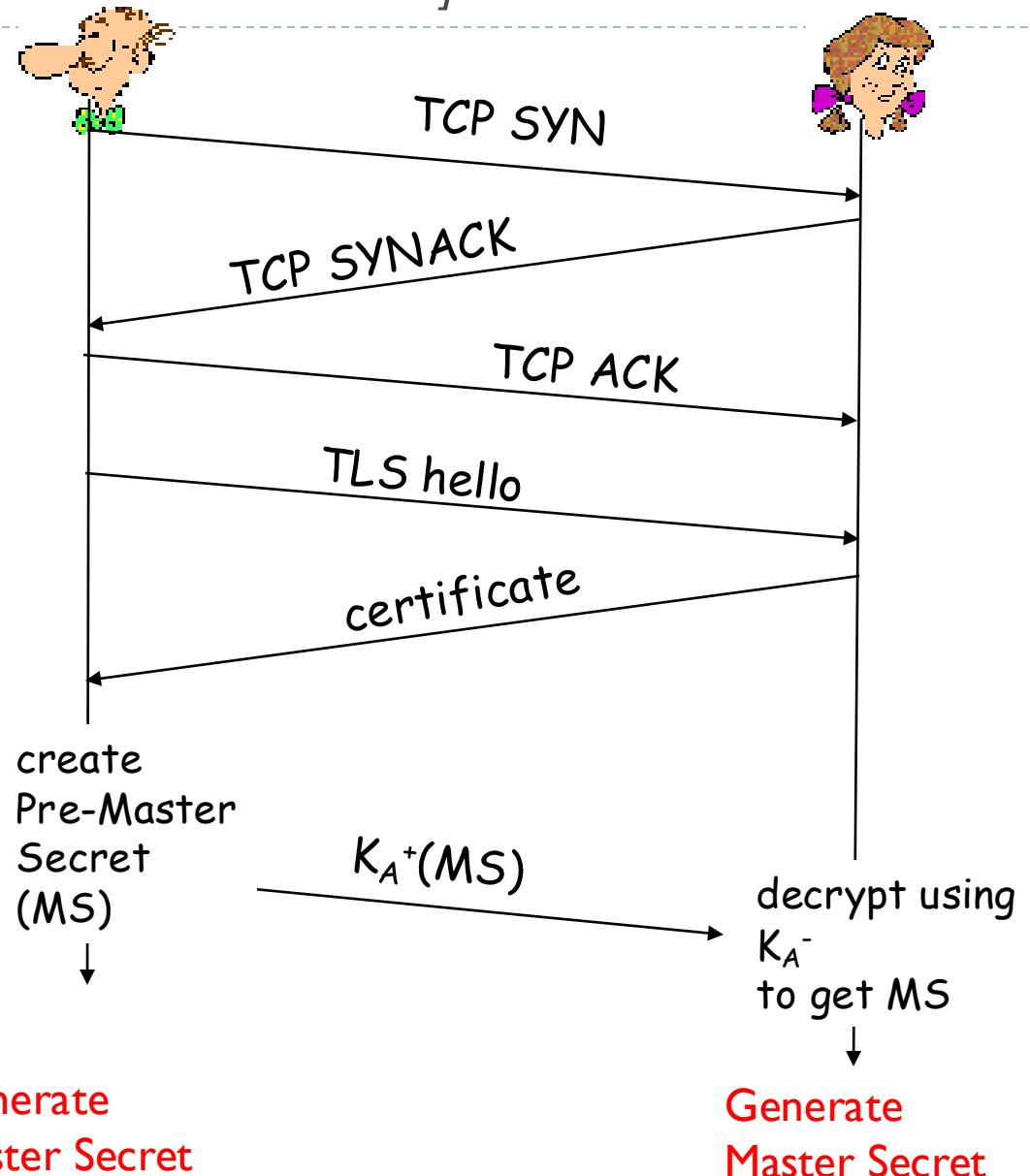
[RSA based key exchange as in ssl and tls < 1.2]

## THREE PHASES

- ▶ Handshake
- ▶ Key Derivation
- ▶ Data Derivation

### Phase I. Handshake:

- ▶ Bob establishes TCP connection to Alice
- ▶ authenticates Alice via CA signed certificate
- ▶ creates, encrypts (using Alice's public key), sends pre-master secret key to Alice



# A toy-TLS Handshake

*[RSA based key exchange as in ssl and tls < 1.2]*

---

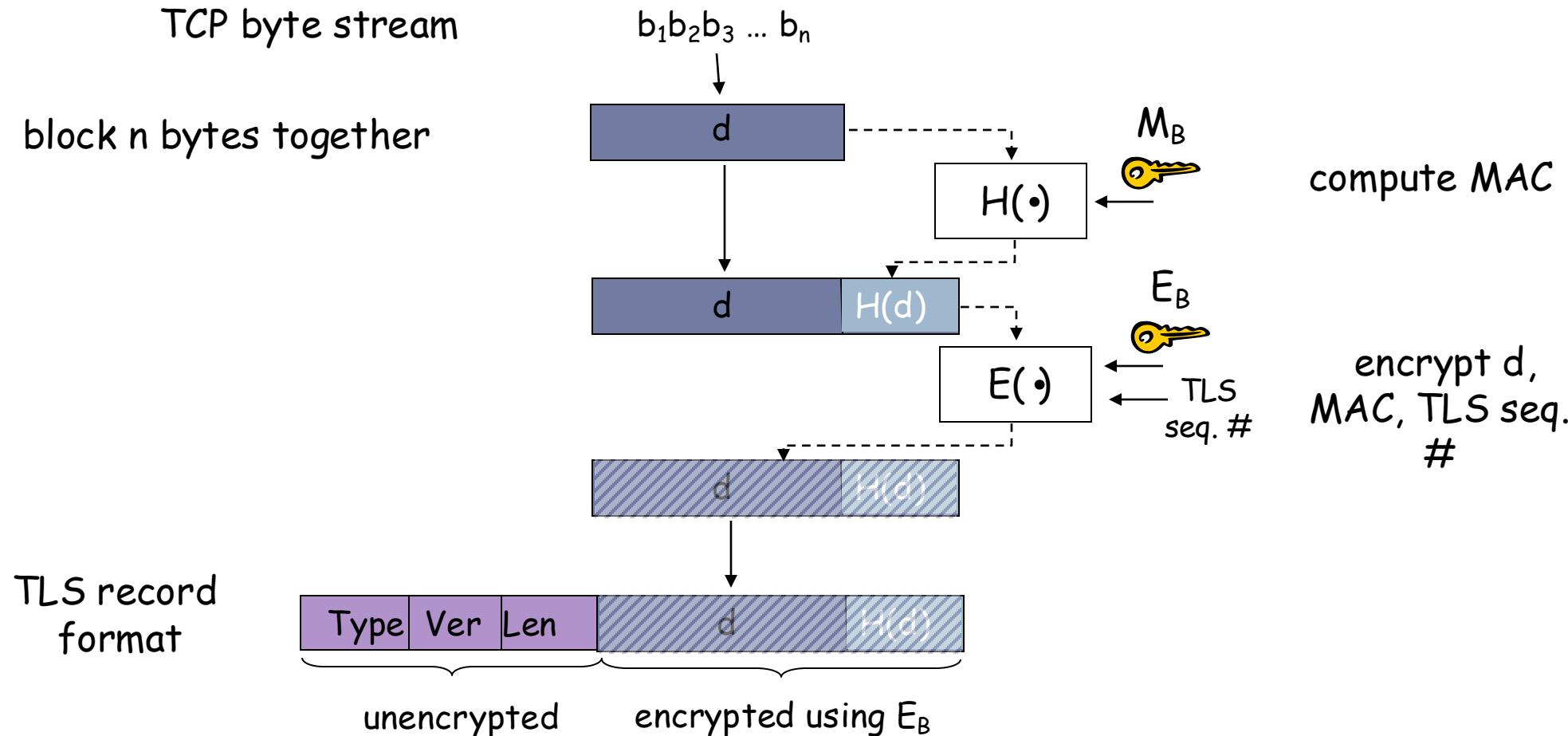
## Phase 2. Key Derivation:

- ▶ Alice, Bob use master secret (MS) to generate 4 keys:
  - ▶  $E_B$ : Bob->Alice data encryption key
  - ▶  $E_A$ : Alice->Bob data encryption key
  - ▶  $M_B$ : Bob->Alice MAC (message authentication code) key
  - ▶  $M_A$ : Alice->Bob MAC key
- ▶ encryption and MAC algorithms negotiable between Bob, Alice
- ▶ **why 4 keys?**



# A toy-TLS Handshake [as in ssl and tls < 1.2]

## Phase 3. Data transfer



# Transport Layer Security (toy TLS): Summary

for your reference!

- ▶ TLS handshake
  1. Client sends cryptography and hash algorithms it supports to server in client **Hello message**
  2. Server selects a symmetric key algorithm, public key algorithm and MAC (hash) algorithm. Sends choices to client with a **certificate** and server nonce.
  3. Client verifies certificate, extracts server's public key and generates **pre-master key(preMS)**. Encrypts the preMS with server's public key. Sends encrypted preMS to server.
  4. Both client and server use the same **key derivation function** to generate MS and the 4 keys from the MS.
  5. Client sends MAC of all handshake messages
  6. Server sends MAC of all handshake messages
- ▶ Connection close
  1. An TLS record with type field set to "close" is sent. Then TCP FIN is sent.
- ▶ Questions to ponder:
  - ▶ What are the four keys derived from MS and their uses?
  - ▶ What is the purpose of message 5 and 6 in TLS handshake?

# TLS: I.3 cipher suite

- ▶ “cipher suite”: algorithms that can be used for key generation, encryption, MAC, digital signature
- ▶ TLS: I.3 (2018): more limited cipher suite choice than TLS I.2 (2008)
  - ▶ only 5 choices, rather than 37 choices
  - ▶ **Key Exchange**: requires Diffie-Hellman (DH) for key exchange, rather than RSA
  - ▶ **Encryption**: Combined encryption and authentication algorithm (“authenticated encryption”) for data rather than serial encryption, authentication.
  - ▶ **Protocol**: Known as Authenticated Key Exchange (AKE) protocol, based on **SIGMA (“SIGn-andMAc”)**
    - ▶ Uses DSS (Digital Signature Standard) for Authentication.
    - ▶ **Integrity**: HMAC uses SHA (256 or 284) cryptographic hash function

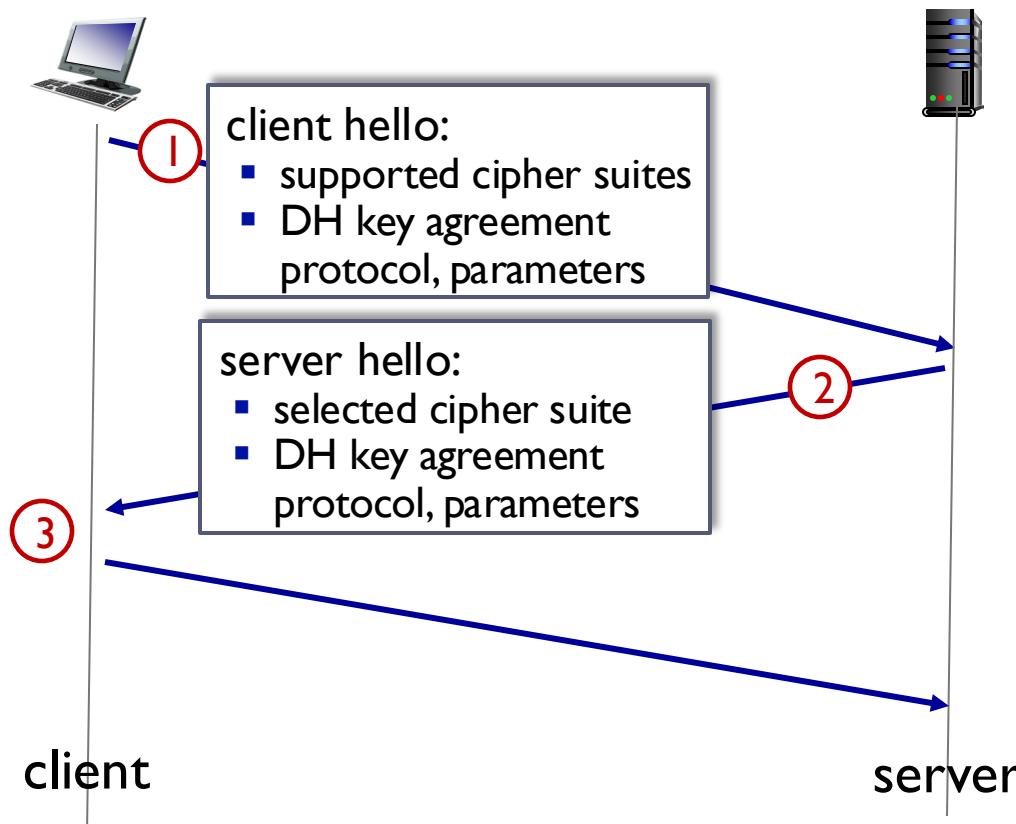
**Original SIGMA paper:** H. Krawczyk. SIGMA: The “SIGn-and-MAc” approach to authenticated Diffie-Hellman and its use in the IKE protocols. In D. Boneh, editor, CRYPTO 2003, volume 2729 of LNCS, pages 400–425. Springer,

# RSA vs DH for Key Exchange

- ▶ Q: Suppose past communications between client and server are stored. If the RSA private key of the server or client is compromised (at any future time), can it be used to decrypt the past communication?

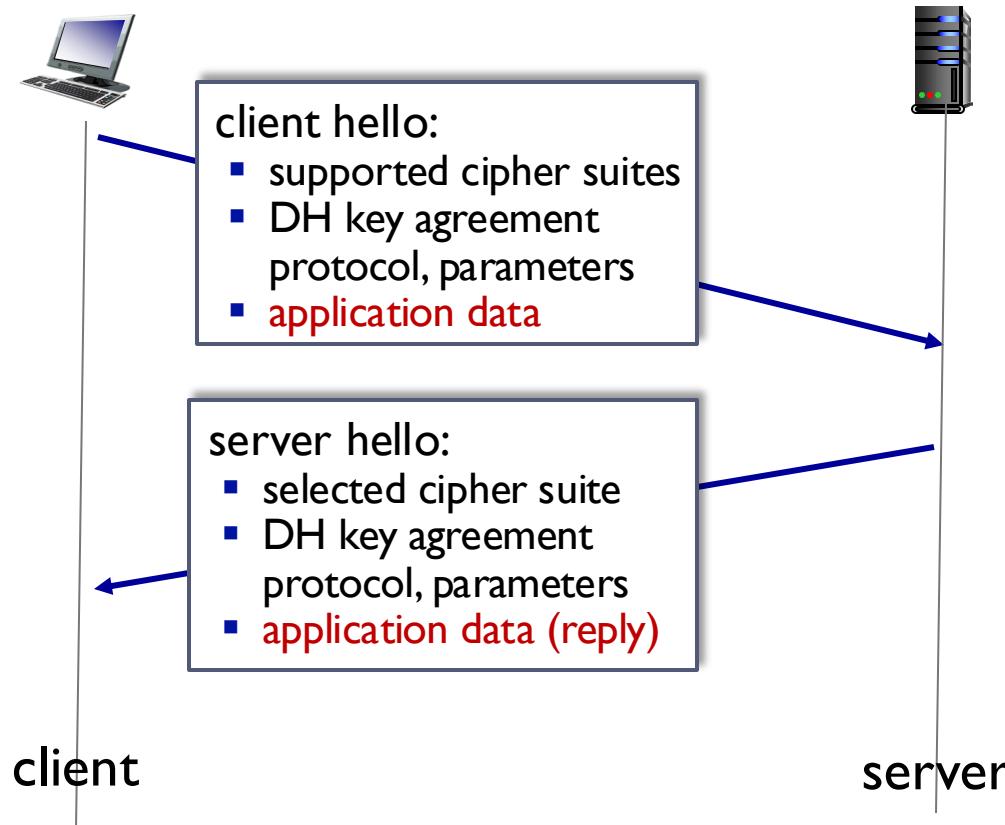


# TLS 1.3 handshake: I RTT



- ① **client TLS hello msg:**
  - guesses key agreement protocol, parameters
  - indicates cipher suites it supports
- ② **server TLS hello msg chooses**
  - key agreement protocol, parameters
  - cipher suite
  - server-signed certificate
- ③ **client:**
  - checks server certificate
  - generates key
  - can now make application request (e.g., HTTPS GET)

# TLS 1.3 handshake: 0 RTT



- ▶ initial hello message contains encrypted application data!
  - “resuming” earlier connection between client and server
  - application data encrypted using “resumption master secret” from earlier connection
- ▶ vulnerable to replay attacks!
  - maybe OK for get HTTP GET or client requests not modifying server state

# Secure E-mail & Pretty good privacy (PGP)

- Internet e-mail encryption scheme, de-facto standard.
- **Options:** signing only, encryption only and both
- uses symmetric key cryptography, public key cryptography, hash function, and digital signature as described.
- provides secrecy, sender authentication, integrity.
- inventor, **Phil Zimmerman**, was target of 3-year federal investigation.
  - ★ US cryptographic sw export restrictions
  - ★ 1991, dropped 1996

A PGP signed message: (appears after the MIME header)

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town tonight.

Passionately yours, Alice

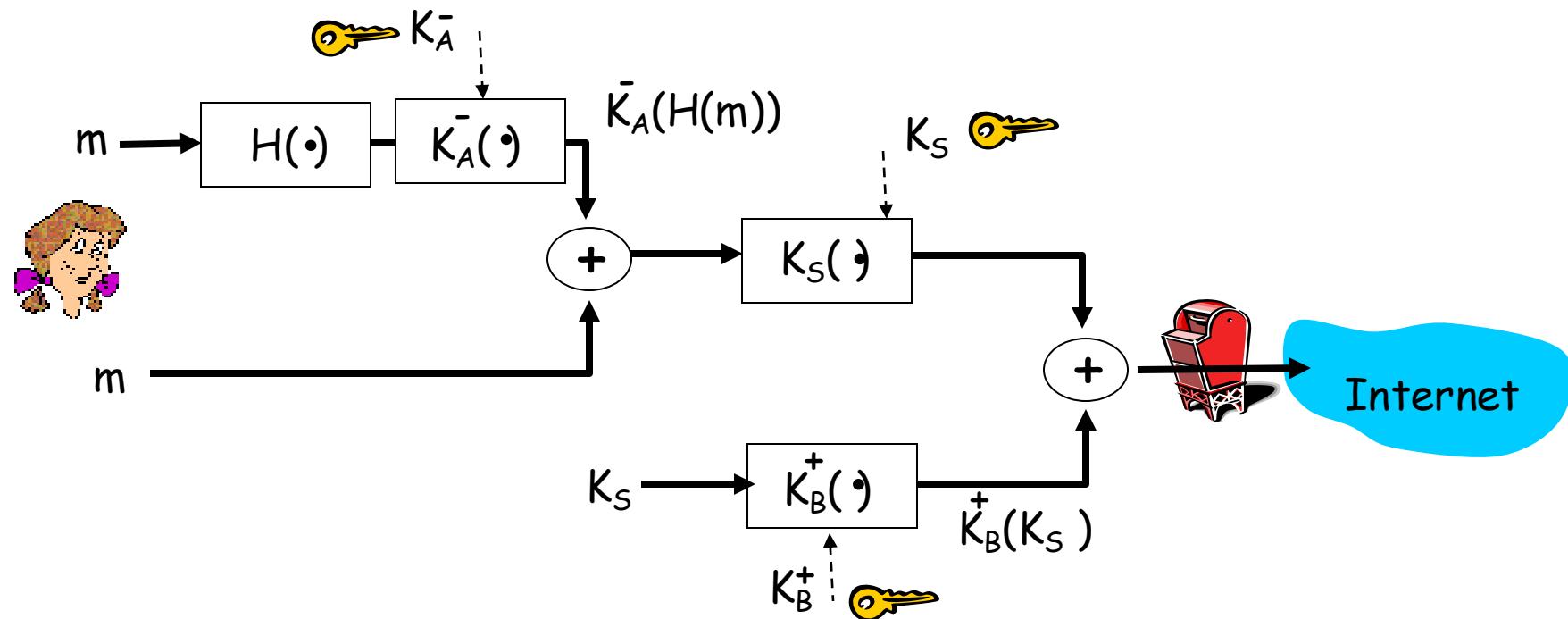
---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yHJRhhGJGhgg/12EpJ+lo8gE4vB3mqJhFEvZP9t6n7
G6m5Gw2
---END PGP SIGNATURE---
```

Note: not encrypted.



# Secure E-mail & Pretty good privacy (PGP)

Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key ( $K_A^-$ ) Bob's public key ( $K_B^+$ ) , newly created symmetric key ( $K_S$ )

# Summary

---

- Attacks on Internet
- Services by a Security System
- Security protocols and algorithms
  - Integrity – hash
  - Authentication – keyed hash (symmetric key), signing the hash with private key
  - Confidentiality – encrypt the message
- Internet Security - Examples
  - TLS, PGP, VPN...

QUESTIONS?

