Unit-3
Access Control System and Methodology and Cryptography

Access control system and methodology

- Access controls are a collection of mechanisms that work together to create security a architecture, to protect the assets of an information system.
- One of the goals of access control is personal accountability, which is the mechanism that proves someone performed a computer activity at a specific point in time.

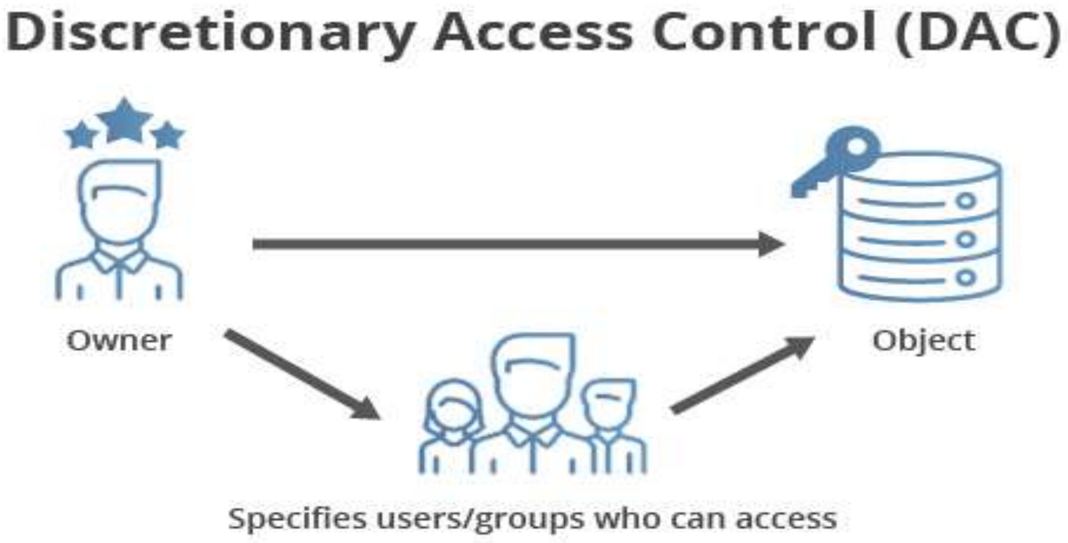
TERMS AND CONCEPTS

- *Identification*
- Identification credentials uniquely identify the users of an information system.
- identification equates to a user’s offline identity through his or her name, initials, or email address, or a meaningless string of characters.
- The identification credentials in terms of how you identify yourself in the offline world: name, social security number, student ID number, and so on.
- ***Authentication***
- Authentication credentials permit the system to verify someone’s identification credential.
- Most often this is a simple password that you set up when you receive the privilege to access a system.
- Your photo authenticates your identity.

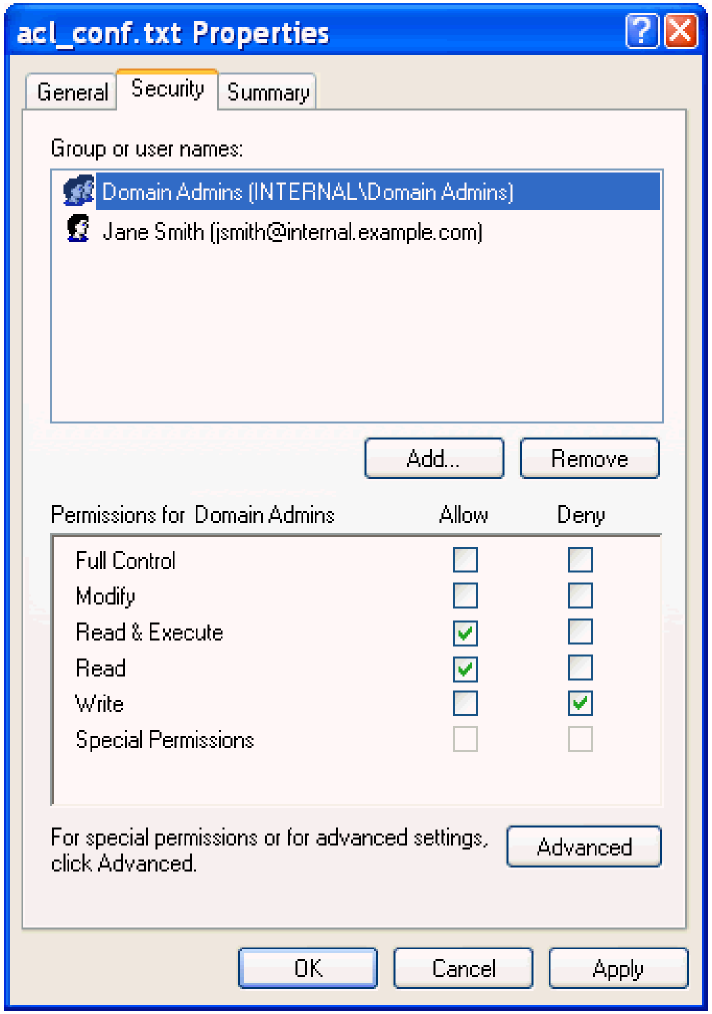
- Another common authentication of your identity is your signature. If your signature matches the signature on your credential, the recipient can be reasonably assured that you are who your ID claims you are.
- ***Least Privilege (Need to Know)***
- The principle of least privilege is the predominant strategy to ensure confidentiality.
- The “need to know” concept governs the privilege (authority) to perform a transaction or access a resource (system, data, and so forth).
- Access is granted only when the subject also has the need to know.

- ***Information Owner***
- An information owner is one who maintains overall responsibility for the information within an information system.
- Who will be information owner in corporate world, academics?
- Information owners can delegate the day-to-day work to a subordinate or to an information technology department, but they cannot delegate the overall responsibility for the information and the system that maintains it.
- The information owner must be the one to make the decisions about who uses the system and how to recover the system in case a disaster.

- ***Discretionary Access Control***
- The principle of discretionary access control (DAC) dictates that the information owner is the one who decides who gets to access the system(s).
- This is how most corporate systems operate.
- DAC authority can be delegated to others who then are responsible for user setup, revocation, and changes (department moves, promotions, and so forth).


Discretionary Access Control (DAC)
Owner
Object
Specifies users/groups who can access

- ***Access Control Lists***
- An access control list (ACL) is simply a list or a file of users who are given the privilege of access to a system or a resource (such as a database).
- Within the file is a user ID and an associated privilege or set of privileges for that user and that resource.
- The privileges are typically Read, Write, Update, Execute, Delete, and Rename.



Group or user names:

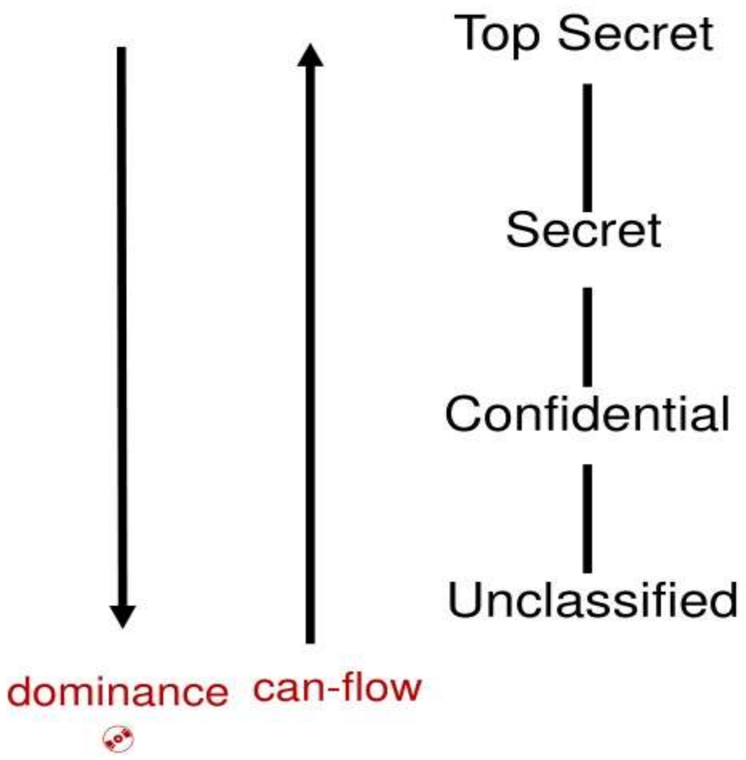
Domain Admins (INTERNAL\Domain Admins)
Jane Smith (jsmith@internal.example.com)

Permissions for Domain Admins	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
Read	☑	□
Write	□	☑
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

- ***User Provisioning***
- The activity of bringing new employees into an organization includes granting them access to the systems that they need to perform their duties.
- User provisioning activities include checking management approvals for granting access.
- User provisioning tools help managers determine what rights their employees possess and to recertify their need for ongoing access periodically.
- ***Mandatory Access Control***
- In a system that uses mandatory access control (MAC; also called nondiscretionary access control), the system decides who gains access to information based on the concepts of subjects, objects, and labels, as defined here.

- In a MAC environment, objects (including data) are labeled with a classification (Secret, Top Secret, and so forth), and subjects, or users, are cleared to that class of access.



Top Secret

Secret

Confidential

Unclassified

dominance

can-flow

Labeling Mechanism is used

Prevent any illegal flow of information through the enforcement of multilevel security

Military Security

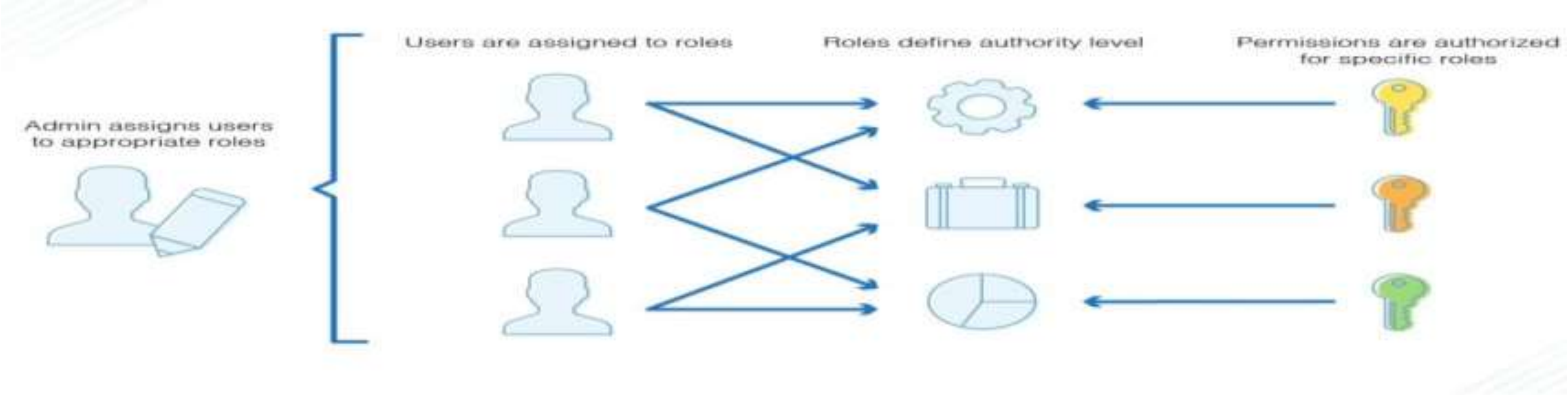
Require a strict classification of subjects and objects in security levels

Drawback of being too rigid

Applicable only to very few environments

- • **Subjects:** The people or other systems that are granted a clearance to access an object within the information system.
- • **Objects:** The elements within the information system that are being protected from use or access.
- • **Labels:** The mechanism that binds objects to subjects. A subject’s clearance permits access to an object based on the labeled security protection assigned to that object.
- For example, only subjects who are cleared to access Secret objects may access objects labeled Secret or less than Secret, provided that they also possess the need to know.

- ***Role-Based Access Control***
- Role-based access control (RBAC) groups users with a common access need.
- You can assign a role for a group of users who perform the same job functions and require similar access to resources.
- Role-based controls simplify the job of granting and revoking access by simply assigning users to a group and then assigning rights to the group for access control purposes.
- This is especially helpful in companies that experience a high rate of employee turnover or frequent changes in employee roles.


Users are assigned to roles
Roles define authority level
Permissions are authorized for specific roles
Admin assigns users to appropriate roles

PRINCIPLES OF AUTHENTICATION

- The idea of authentication is that only the legitimate user possesses the secret information needed to prove to a system that he or she has the right to use a specific user ID. These secrets are commonly passwords, but history shows that passwords are problematic.

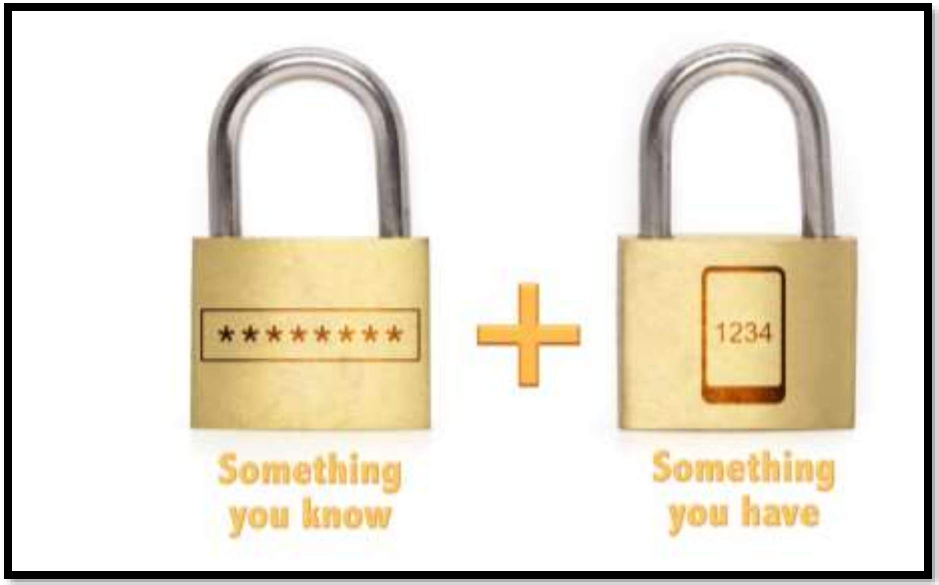
The Problems with Passwords

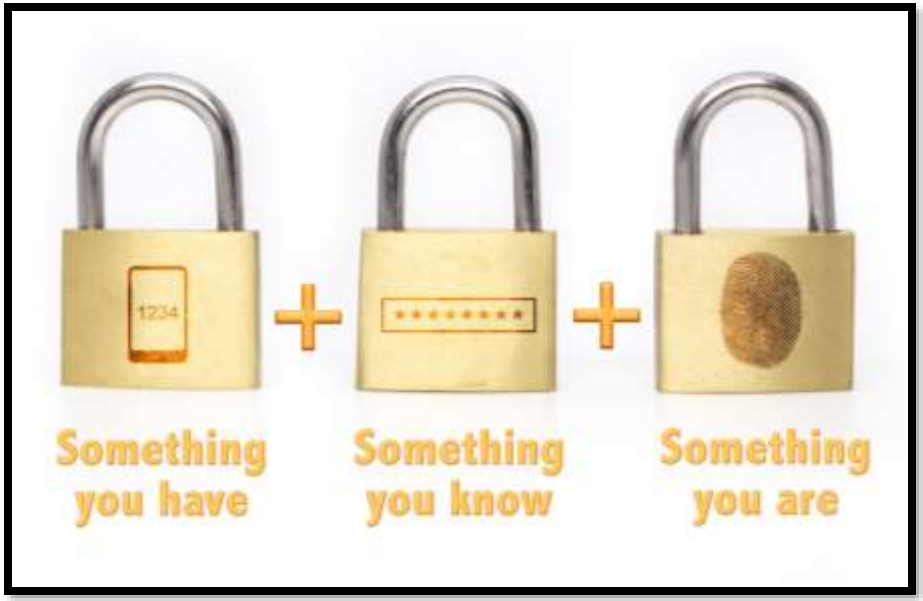
- • **Passwords can be insecure.** Given the choice, people will choose easily remembered and easily guessed passwords, such as names of relatives, pets, phone numbers, birthdays, hobbies, and other similar items.
- • **Passwords are easily broken.** Common words in an ordinary dictionary make for poor choices of passwords. Free and widely available programs are available on the Internet to crack passwords through a dictionary attack.
- Passwords are an example of single-factor authentication, which is simply something someone knows that is used to gain access to a system with no further requirements for proving identity.

Multifactor Authentication

- With two or three factors (multifactor authentication) to authenticate, an information owner can gain confidence that users who access their systems are indeed authorized to access those systems.
- 1. **Two-Factor Authentication**
- With a two-factor authentication system, a user has a physical device (a card, token, smart card, USB flash drive, and so forth) that contains his or her credentials, protected by a personal identification number (PIN) or a password that the user keeps secret.
- This condition is described as something you have plus something you know (SYH/SYK).
- An example is your debit card and PIN used to access an automated teller machine (ATM) at your bank. The card identifies you as the account holder, and the PIN authenticates you to the device.

- 2. **Three-Factor Authentication**
- In a three-factor system, unique information related to the user is added to the two-factor authentication process.
- This unique information might be a biometric (fingerprint, retinal scan, and so forth) needed for authentication.
- The three-factor mechanism is described as something you have plus something you know plus something you are (SYH/SYK/SYA).


****
1234
Something you know
Something you have


1234
****
Something you have
Something you know
Something you are

BIOMETRICS

- Biometric methods of identification work by measuring unique human characteristics as a way to confirm identity. The following are common biometric techniques in use today:
- Fingerprint recognition
- Signature dynamics
- Iris scanning
- Retina scanning
- Voice prints
- Face recognition

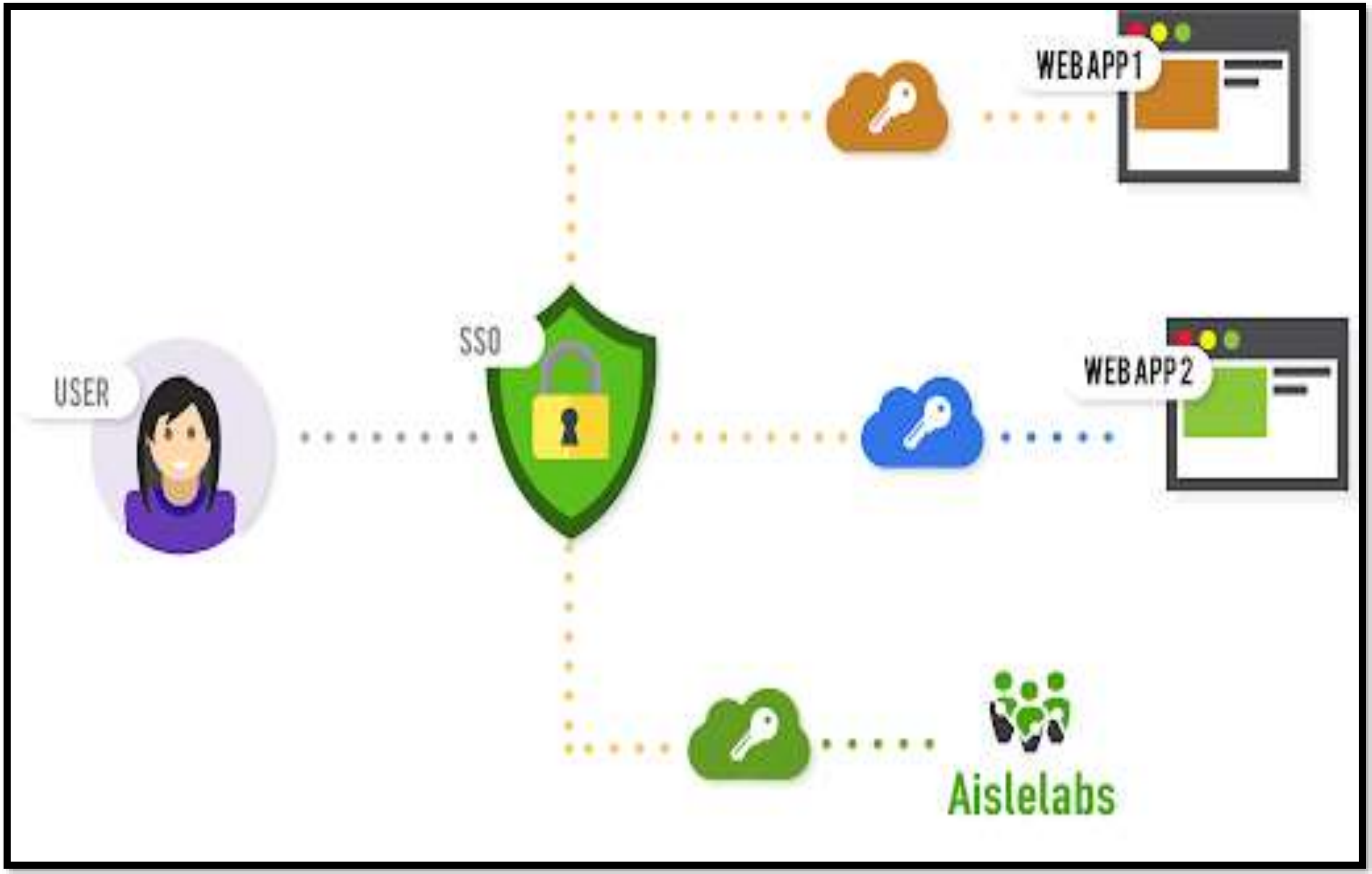
- The most common biometric in use is fingerprint recognition. Consider some advantages of fingerprints:
- Fingerprints can’t be forgotten like a password.
- Fingerprints are a good compromise in ease of use, cost, and accuracy.
- Fingerprints last virtually forever
- Fingerprints make network login and authentication effortless.

Applications:

- • Handling network access control
- • Tracking staff time and attendance
- • Authorizing financial transactions
- • Distributing government benefits
- • Verifying identities at point of sale
- • Working in conjunction with ATM cards, credit cards, or smart cards
- • Controlling physical access to office buildings or homes
- • Protecting personal property
- • Preventing kidnapping in schools, play areas, and other locations

SINGLE SIGN-ON

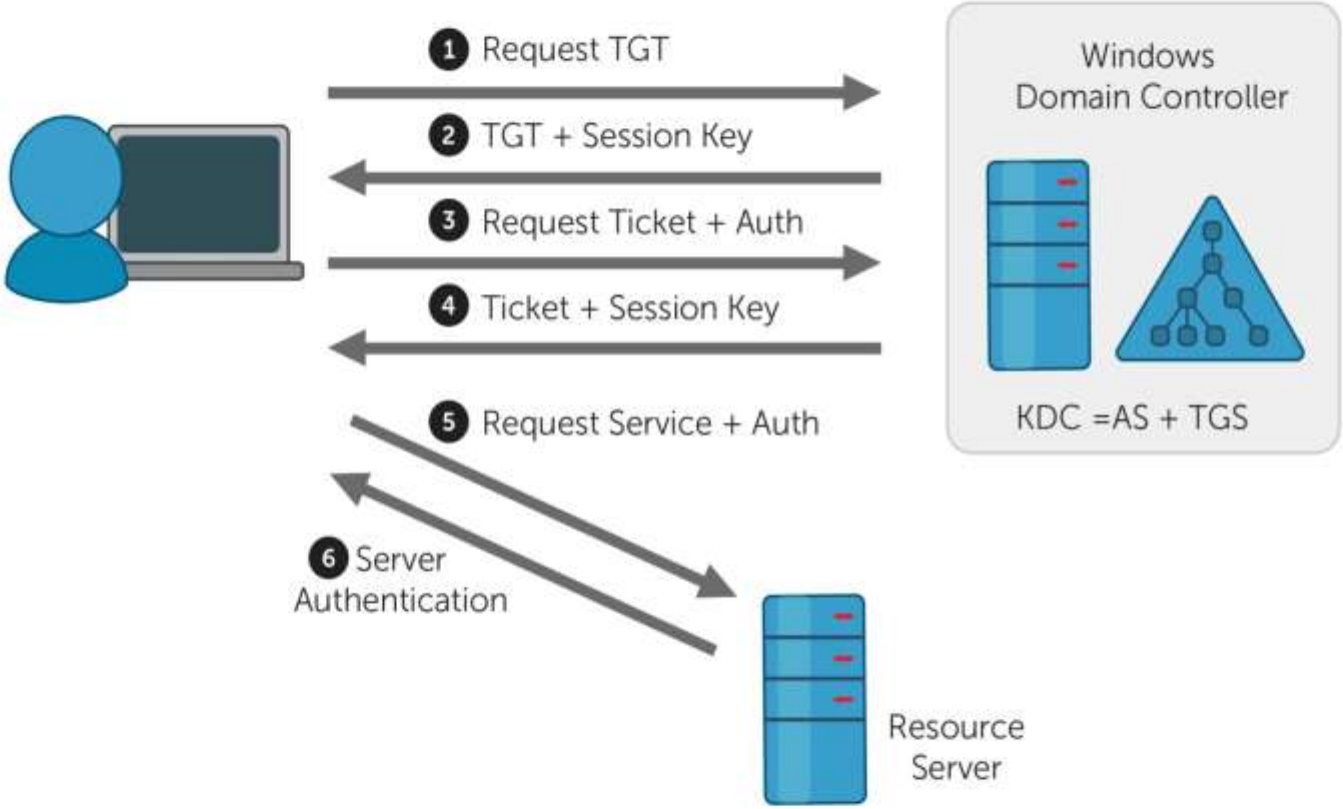
- All the methods to authenticate described in this chapter assume that every system a user needs access to requires a unique ID and password, thus requiring the user to maintain a number of ID/password pairs.
- In an SSO system, users have one password for all corporate and back-office systems and applications that they need to perform their jobs.
- That way, they can remember and use one consistent password, thus increasing the security of the overall system of access controls.
- One common approach to managing IDs and passwords is to create a password or PIN vault.
- Some mechanisms used to implement single sign-on include Kerberos , proprietary mechanisms that mimic Kerberos, and custom-developed solutions that actually maintain the discrete IDs and passwords.


WEB APP 1
SSO
USER
WEB APP 2
Aislelabs

Kerberos

- Kerberos is a network authentication protocol named for the three-headed dog that guarded the entrance to Hades in Greek mythology.
- Kerberos is designed to provide authentication for client/server applications by using symmetric key cryptography.
- The Kerberos protocol uses robust cryptography so that a client can prove his or her identity to a server (and vice versa) across an insecure network connection, such as the Internet.
- After a client and server have used Kerberos to prove their identities, they can also encrypt all their communications to ensure privacy and data integrity as they go about their business.

- Kerberos works by assigning a unique key, called a ticket, to each user who logs on to the network.
- The ticket is then embedded in messages that permit the receiver of the message (programs or other users) to positively identify the sender of the message.
- When using Kerberos, users needs to log in only once, and each resource they want to access checks their tickets for currency and validity when a request for access is made.


1 Request TGT
2 TGT + Session Key
3 Request Ticket + Auth
4 Ticket + Session Key
5 Request Service + Auth
6 Server Authentication
Windows Domain Controller
KDC =AS + TGS
Resource Server

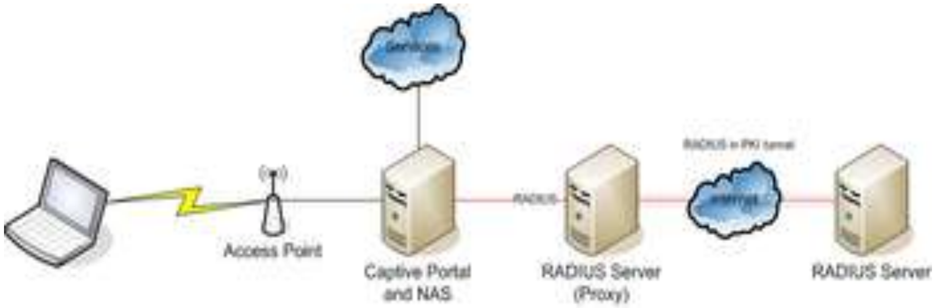
REMOTE USER ACCESS AND AUTHENTICATION

- When working at remote locations or telecommuting from home, additional security problems arise because of the use of insecure networks (such as the Internet) to create a connection to the corporate local area network (LAN).
- Addressing these problems requires additional access control mechanisms to protect both the LAN and the users.

1. ***Remote Access Dial-In User Service***

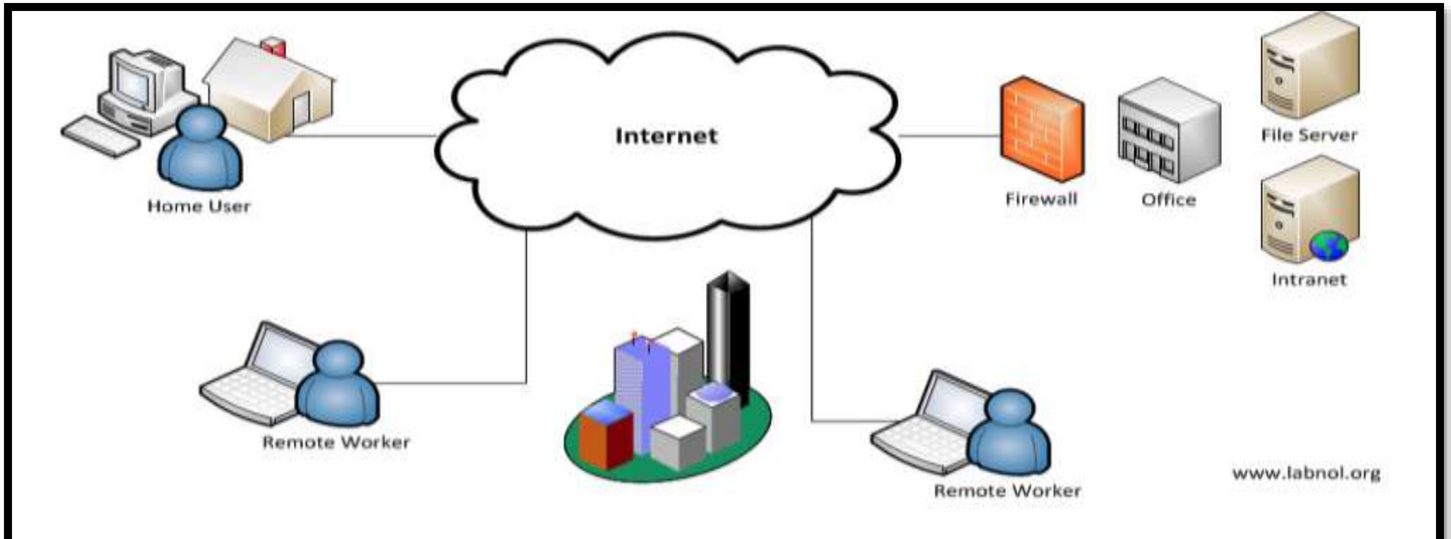
- Remote Access Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access users to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.
- RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.
- RADIUS allows a company to set up a policy that can be applied at a single administered network point.
- Authenticating to a RADIUS server might require using an ID/password combination or, more often, a token or smart card for multifactor

authentication.



2. Virtual Private Networks

- A virtual private network (VPN) is the more common means for remote users to access corporate networks.
- With a VPN, a user connects to the Internet via his or her ISP and initiates a connection to the protected network, creating a private tunnel between the endpoints that prevents eavesdropping or data modification.
- VPNs often use strong cryptography to both authenticate senders and receivers of messages and to encrypt traffic so that it's invulnerable to a man-in-the-middle (MitM) attack.



Cryptography

- **BASIC TERMS AND CONCEPTS**
- A cryptosystem disguises messages, allowing only selected people to see through the disguise.
- Cryptography is the science (or art) of designing, building, and using cryptosystems.
- Cryptanalysis is the science (or art) of breaking a cryptosystem.
- Cryptology is the umbrella study of cryptography and cryptanalysis.

Cryptographers rely on two basic methods of disguising messages: transposition, in which letters are rearranged into a different order, and substitution, in which letters are replaced by other letters and/or symbols.

Plain text is the message that is passed through an encryption algorithm, or cipher—it becomes cipher text. When cipher text is passed through a decryption algorithm, it becomes plain text again.

STRENGTH OF CRYPTOSYSTEMS

- A strong cryptosystem is considered strong only until it’s been cracked.
- Strong cryptosystems produce ciphertext that always appears random to standard statistical tests.
- They also resist all known attacks on cryptosystems and have been brutally tested to ensure their integrity.
- Cryptosystems that have not been subjected to brutal testing are considered suspect.

- **In Practice: A Simple Transposition Encryption Example**
- Although a firm grasp of the actual mechanics of cryptosystems is not directly required to understand how they are used in securing systems, some understanding of the complexities involved helps you appreciate what is going on behind the curtain.
- Using the transposition technique with a symmetric key (shared secret), we can take a look at how encryption and decryption might operate manually.
- Assume that this is the plain text message you want to encrypt:
- SECURITY BEGINS WITH YOU
- You choose the word TEACUPS as your keyword (secret key) and send it to your intended recipient using a secure channel other than the one you will use to send the message. This is for added security and to ensure that the recipient has the key when the ciphertext arrives.
- Encrypt the message through the following steps:
- **1.** Write the key horizontally as the heading for columns:
- T E A C U P S

- **2.** Assign numerical values to each letter, based on the letter’s order of appearance in the alphabet: A=1, C=2, and so on.

T	E	A	C	U	P	S
6	3	1	2	7	4	5

- **3.** Align the plain-text message across each key/value column heading, skipping to the next line when you reach the last column of the matrix.

T	E	A	C	U	P	S
6	3	1	2	7	4	5
S	E	C	U	R	I	T
Y	B	E	G	I	N	S
W	I	T	H	Y	O	U

- **4.** Read down along each column according to the ordinal value of the column to produce the cipher text (A-1 is the first column, C-2 is the second, and so forth):

  CET UGH EBI INO TSU SYW RIY

- **5.** Sender don’t need to worry about it getting into the wrong hands.

- Upon receipt of the cipher text, the recipient decrypts it through the following steps:
- **1.** Write the key horizontally as the heading for columns:

  T E A C U P S
- **2.** Assign numerical values to each letter, based on the letter's order of appearance in the alphabet.

T	E	A	C	U	P	S
6	3	1	2	7	4	5

- **3.** Transpose the cipher text, three letters at a time, using the ordinal value of each column to determine its placement. Because A is column value 1, the first group of letters, CET, is written vertically under A-1. Group 2 belongs under C-2, and so forth:

T	E	A	C	U	P	S
6	3	1	2	7	4	5
S	E	C	U	R	I	T
Y	B	E	G	I	N	S
W	I	T	H	Y	O	U

- **4.** Read the message horizontally to reveal the plain-text message:

  SECURITY BEGINS WITH YOU

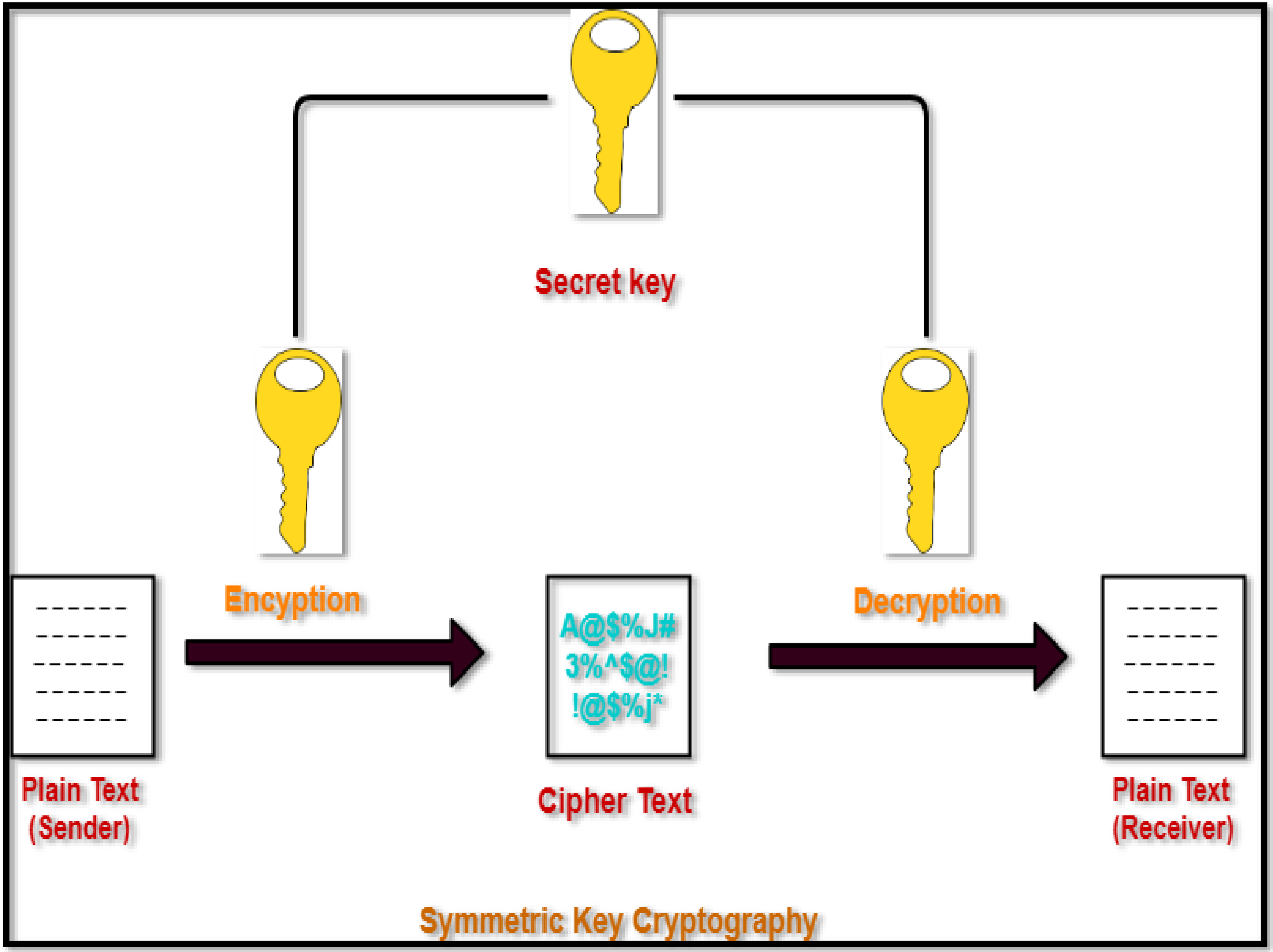
The Role of Keys in Cryptosystems

- Keys (secrets) used for encryption and decryption come in two basic forms, symmetric and asymmetric.
- This simply means that either the same key is used to both encrypt and decrypt, or a pair of keys is needed.
- When the same key is used to both encrypt and decrypt messages, it’s called symmetric key or shared secret cryptography.
- When different keys are used, it’s called asymmetric key cryptography.

- The following is an example of how to convert plain text to cipher text using ROT13.
- **1.** Write down the alphabet, splitting it across two rows in the middle:
- 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
- With the plain-text message THE BUTLER DID IT,
- One major advantage of ROT13 over other Caesar rotation values is that it is self-inverse, so the table shown works for encoding and decoding.

Symmetric Keys

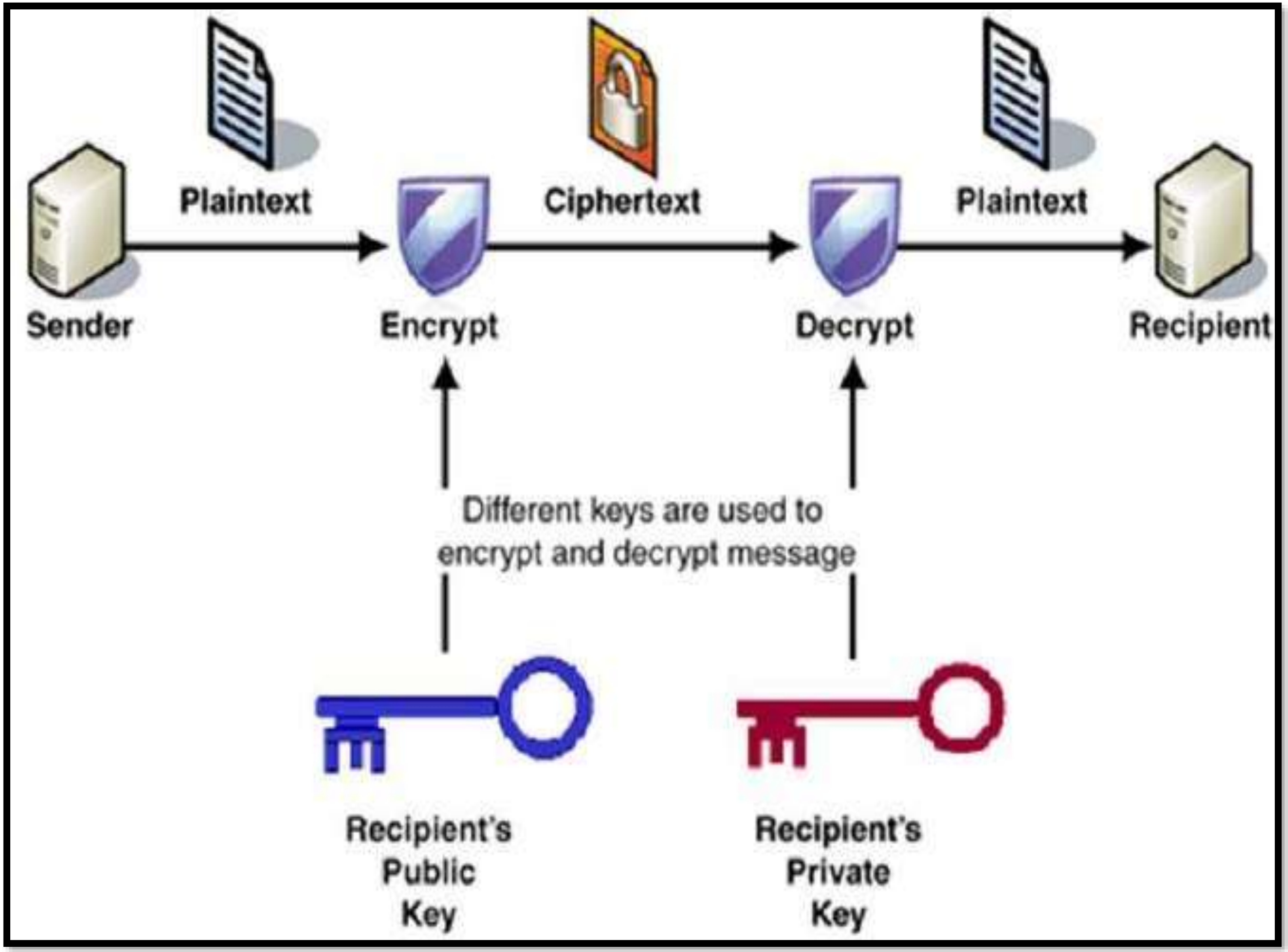
- When you use the same key to both encrypt and decrypt a message, it’s called symmetric key cryptography.
- The most common form of symmetric key cryptography is the Data Encryption Standard.
- It uses 64 bits of data (8 bytes) with a 56-bit (7 byte) key within it.
- Triple DES (3DES) is identical but uses a double-length key (128 bits) that encrypts, then encrypts, and then encrypts again (called “folding” in crypto-speak).
- Banks commonly use 3DES to protect your PIN number when you enter it at an ATM or on a point-of-sale keypad


Secret key
Encyption
Decryption
A@$%J#
3%^$@!
!@$%j*
Plain Text
(Sender)
Cipher Text
Plain Text
(Receiver)
Symmetric Key Cryptography

Asymmetric Keys

- With asymmetric key cryptography, two keys are needed.
- A message encrypted using one key can be decrypted only using the other, and vice versa.
- One key is called a public key, and the other is called a private key.
- the private key must always remain private and must never be shared or copied from where it was generated.
- Using asymmetric key cryptography, you share your public key with everyone you want to communicate with privately, but you keep your private key secret.

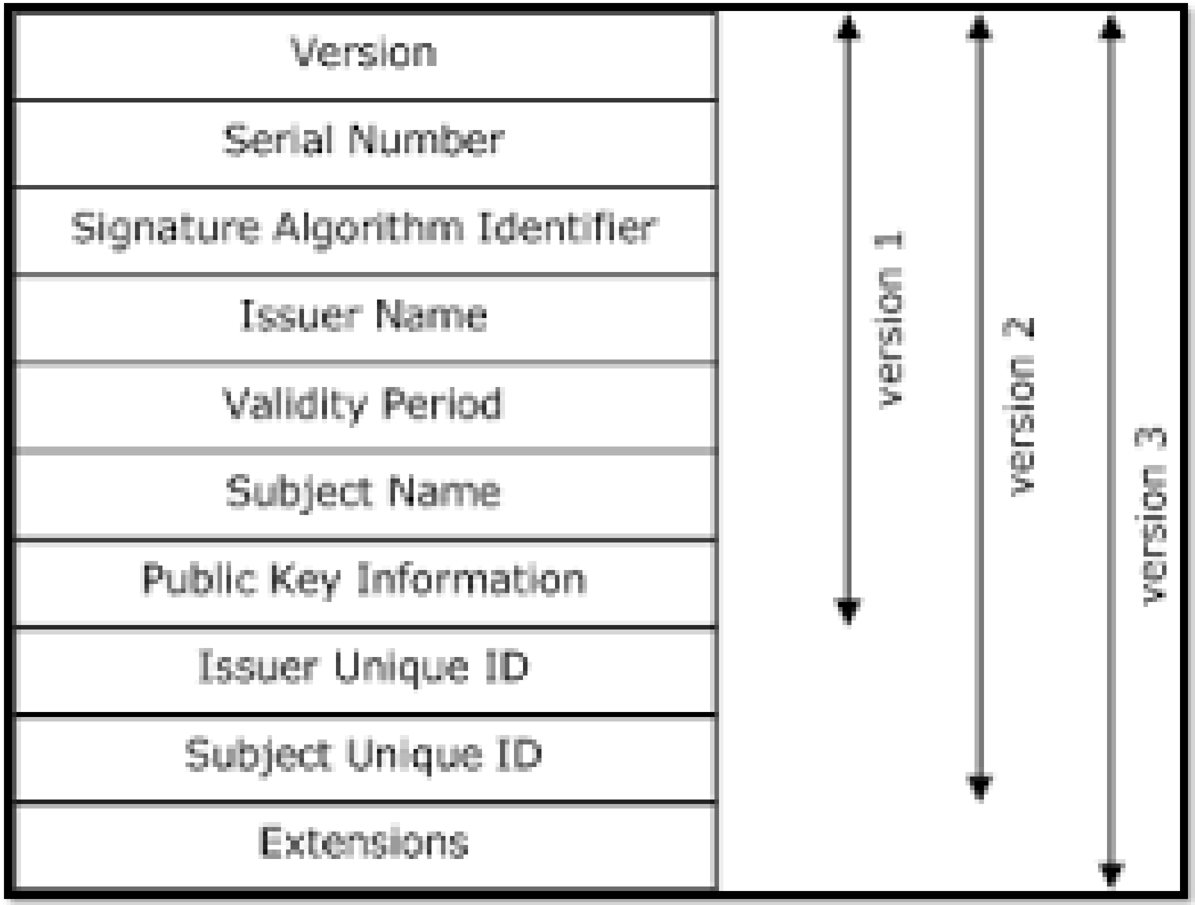
- Your private key essentially is your identity—when someone can successfully decrypt a message that you sent encrypted with your private key, they know that the message could have come from only you if the decryption using the public key succeeds.
- Typically, the keys used with strong asymmetric key cryptography are 1024 bits long (128 bytes) and are meant to foil a brute-force attack on messages.
- PPK cryptography enables you to communicate over any open channel with high degrees of confidence and permits you to trust in these ways:
- • **Authentication:** Messages you receive came from their advertised source.
- • **Privacy:** Messages you send can be read only by their intended receiver(s).
- • **Message integrity:** All messages sent and received arrived intact.


Plaintext
Ciphertext
Plaintext
Sender
Encrypt
Decrypt
Recipient
Different keys are used to encrypt and decrypt message
Recipient's Public Key
Recipient's Private Key

Digital Certificates

- Digital certificates behave in the online world the same way driver’s licenses, passports, and other trusted documents behave beyond the online world.
- The digital certificate standard X.509 governs how certificates are constructed and used between communicating parties.
- When used for signing electronic messages (creating digital signatures), the private key associated with the public key in the digital certificate creates the unforgeable fingerprint (digest) for the message.
- X.509 certificates are similar to notary seals—they bind a person’s identity to a pair (or pairs) of cryptographic keys.

- Digital certificates are issued by a trusted party, called a certificate authority, or CA.
- These CAs operate on behalf of those who want to operate a public key infrastructure (PKI) using X.509 recommended standards.



Version

Serial Number

Signature Algorithm Identifier

Issuer Name

Validity Period

Subject Name

Public Key Information

Issuer Unique ID

Subject Unique ID

Extensions

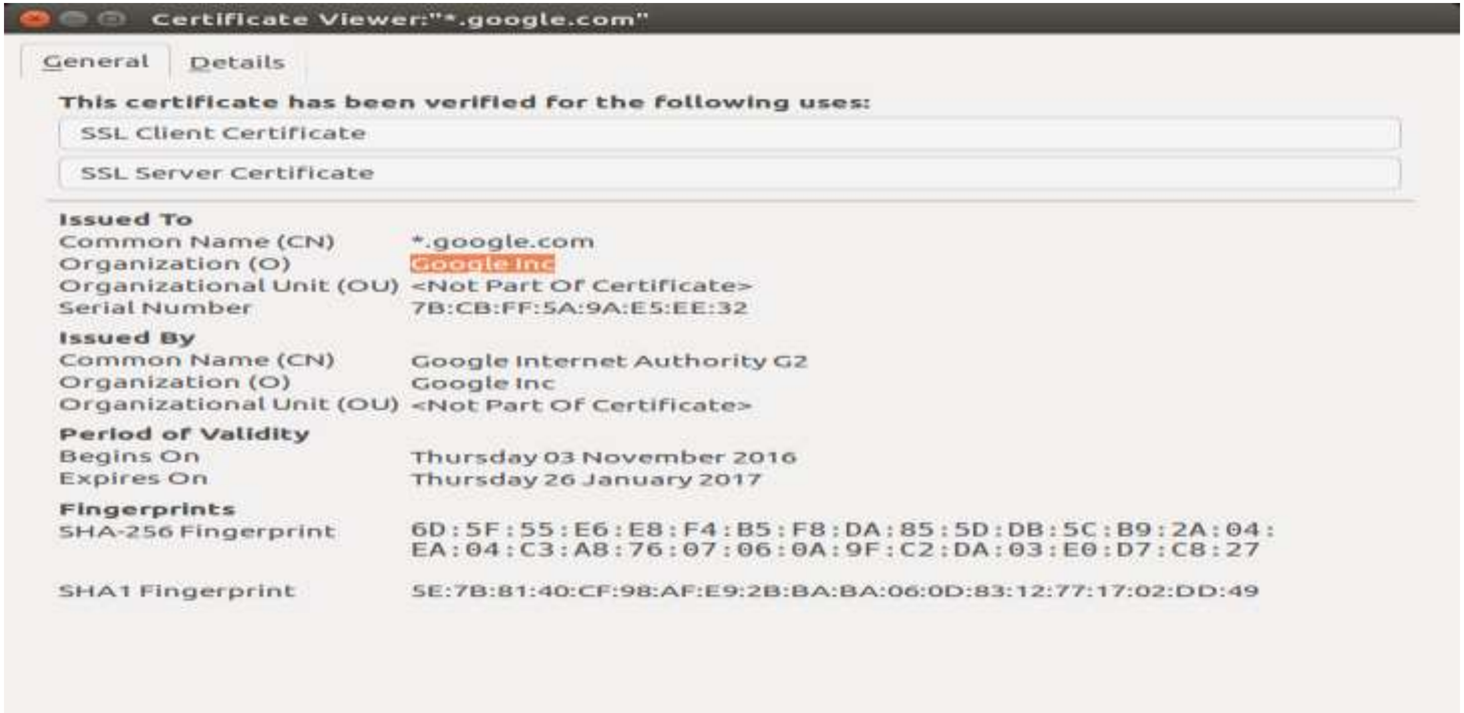
version 1

version 2

version 3

- Each certificate is issued for specific uses and with guidelines described within the certificate’s extensions.
- Extensions can be labeled as critical, mandatory, or optional, depending on the issuer’s requirements.
- CAs maintain a tree of trust that’s checked each time a certificate is presented as proof of one’s identity.
- When the tree of trust is successfully traversed, the recipient can ascertain proof of identity and proof of a person’s right to use the key.
- Many of the higher-order e-commerce protocols, such as Secure Sockets Layer (SSL), use a robust set of digital certificates to authenticate people and resources, to ensure that all parties possess the rights needed to transact.

- Using digital certificates offers system users high degrees of security along several dimensions of communications.
- Because of the cryptography used to process messages, anyone receiving a signed message, along with the public key in the sender's digital certificate, can be confident that the message came from the specific person (user authentication) and that the message itself arrived intact (integrity).



This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To	
Common Name (CN)	*.google.com
Organization (O)	Google Inc
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	7B:CB:FF:5A:9A:E5:EE:32
Issued By	
Common Name (CN)	Google Internet Authority G2
Organization (O)	Google Inc
Organizational Unit (OU)	<Not Part Of Certificate>
Period of Validity	
Begins On	Thursday 03 November 2016
Expires On	Thursday 26 January 2017
Fingerprints	
SHA-256 Fingerprint	6D:5F:55:E6:E8:F4:B5:F8:DA:85:5D:DB:5C:B9:2A:04: EA:04:C3:A8:76:07:06:0A:9F:C2:DA:03:E0:D7:C8:27
SHA1 Fingerprint	5E:7B:81:40:CF:98:AF:E9:2B:BA:BA:06:0D:83:12:77:17:02:DD:49

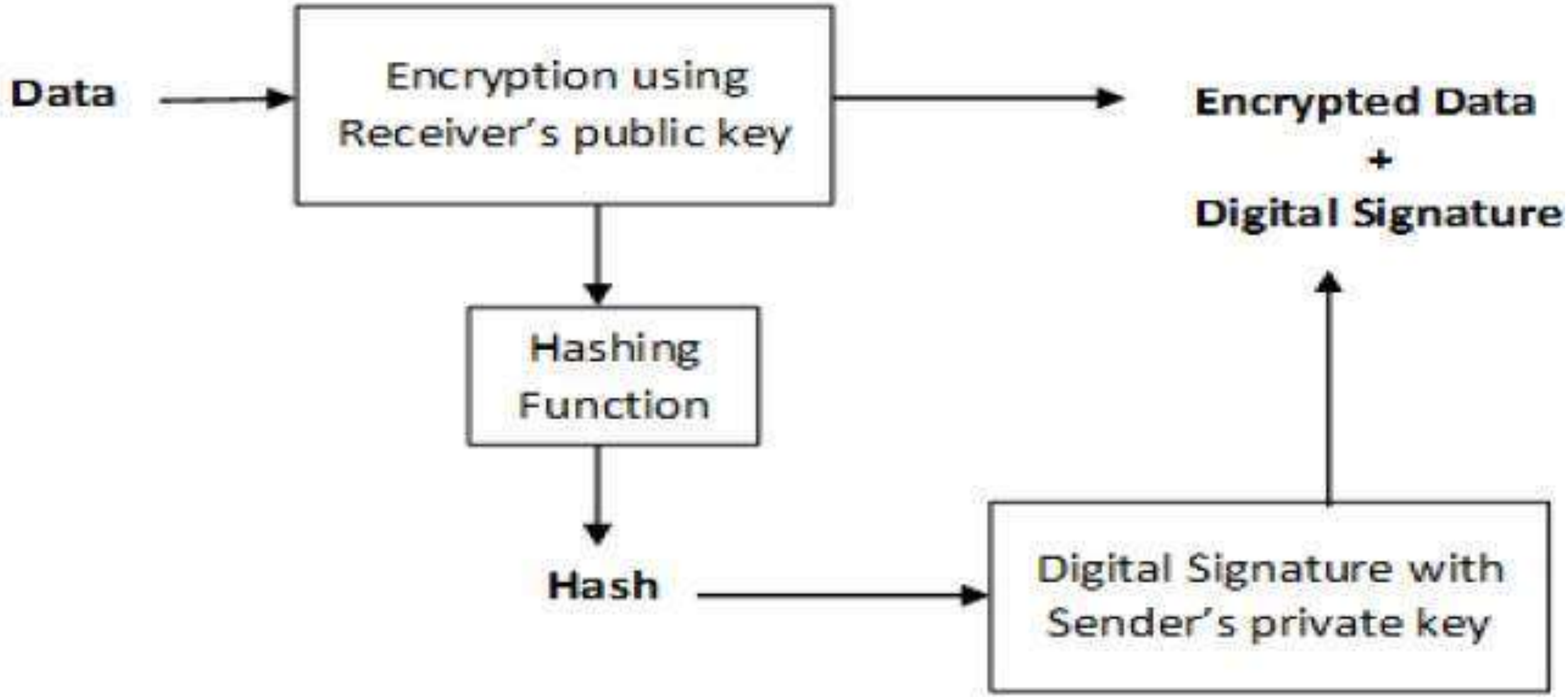
EXAMINING DIGITAL CRYPTOGRAPHY

- Several types of cryptosystems have come into the mainstream over the years. The most significant categories follow:
- Hashing functions (SHA-1 and SHA-3)
- Block ciphers (DES, 3DES, and AES)
- Implementations of RSA Public-Private Key (PPK)

1. Hashing Functions

- you’ve seen some of the most common hashing functions to create the message digest for digitally signed messages
- Hashing-type functions can also be used with symmetric key cryptography; the result of the operation is called a message authentication code, or MAC.
- Hashing is a powerful mechanism for protecting user passwords.
- If a system requires IDs and passwords for any reason, it is best to store the passwords people create in the form of a hash value.
- The Secure Hashing Algorithm (SHA) variants are the most common forms of hashing functions you’ll encounter with most commercial software.

Sender’s Side



Data

Encryption using Receiver’s public key

Encrypted Data + Digital Signature

Hashing Function

Hash

Digital Signature with Sender’s private key

2. Block Ciphers

- Earlier, you read about DES, Triple-DES, and AES as the most common forms of symmetric key block cipher cryptosystems.
- DES uses a 56-bit (7 bytes plus a checksum byte) key, which is considered weak today.
- Triple DES uses a 112-bit (14 bytes plus 2 checksum bytes) key, and AES uses a variable-length key (256 bits, 512 bits, and so on).
- Block ciphers are important for encrypting/decrypting data in bulk, such as files or batches of data.
- Block ciphers can be used to encrypt data fields (attributes) in records and tables, entire records of data, or entire files or database tables.

3. Implementations of PPK Cryptography

- Public-private key cryptography has found its way into numerous implementations intended to better secure Internet communications and prove identities, including these systems:
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- Pretty Good Privacy (PGP)
- Secure Multipurpose Internet Mail Extensions (S/MIME)
- Secure Electronic Transactions (SET)

3.1 The Secure Sockets Layer Protocol

- SSL was designed for client/server applications, to prevent the unwanted tampering of data transmission, whether eavesdropping, data alteration, or message forgery.

3.2 The Transport Layer Security Protocol

- The Transport Layer Security (TLS) protocol is designed to provide communications privacy over the Internet.
- The goals of TLS protocols are to provide the following:
- • **Cryptographic security:** TLS should be used to establish a secure connection between two parties.
- • **Interoperability:** Independent programmers should be able to develop applications using TLS that can then successfully exchange cryptographic parameters without knowing one another's code.
- • **Extensibility:** TLS seeks to provide a framework into which new public key and bulk encryption methods can be incorporated as necessary. This also accomplishes two subgoals: It prevents the need to create a new protocol, which would risk the introduction of possible new weaknesses, and it avoids the need to implement an entire new security library.
- • **Relative efficiency:** Cryptographic operations, particularly public key operations, tend to be highly CPU intensive. For this reason, the TLS protocol has incorporated an optional session caching scheme to reduce the number of connections that need to be established from scratch. Additionally, care has been taken to reduce network activity.

3.3 The Pretty Good Privacy Protocol

- Pretty Good Privacy (PGP) is a distributed key-management approach that does not rely on certificate authorities.
- PGP is often used to encrypt documents that can be shared via email over the open Internet.
- Users of PGP password-protect the file, the password is used in the process of encryption,

3. 4 The Secure/Multipurpose Internet Mail Extensions Protocol

- Secure/Multipurpose Internet Mail Extensions (S/MIME) offers another standard for electronic mail encryption and digital signatures.
- if Person A uses a web browser that supports S/MIME and tries to communicate with Person B, who uses a different browser supported by PGP, the two individuals most likely will not be able to communicate successfully.

3.5 The Secure Electronic Transactions Protocol

- Secure Electronic Transactions (SET) was designed to address most of the consumer demands for privacy when using a credit card to shop online.
- SET uses are specific to the payment acceptance phases of the shopping experience.
- SET was designed to use a robust set of strictly controlled digital certificates to identify cardholders, merchants, and acquiring payment gateways, to ensure the security of messages passing through open channels such as the Internet.

Questions

- 1. Explain Identification, Authentication, least privilege.
- 2. Discuss DAC, MAC, RBAC, ACL.
- 3. Explain types of authentication.
- 4. Explain SSO.
- 5. What is Kerberos?
- 6. Explain methods of remote user access.(RADIUS, VPN)
- 7. What is cryptography? Explain Symmetric key and asymmetric key cryptography.
- 8. Write a short note on Digital Signature.