Certificates and Authentication

COMP620 Information Privacy and Security

“Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.”

Clifford Stoll

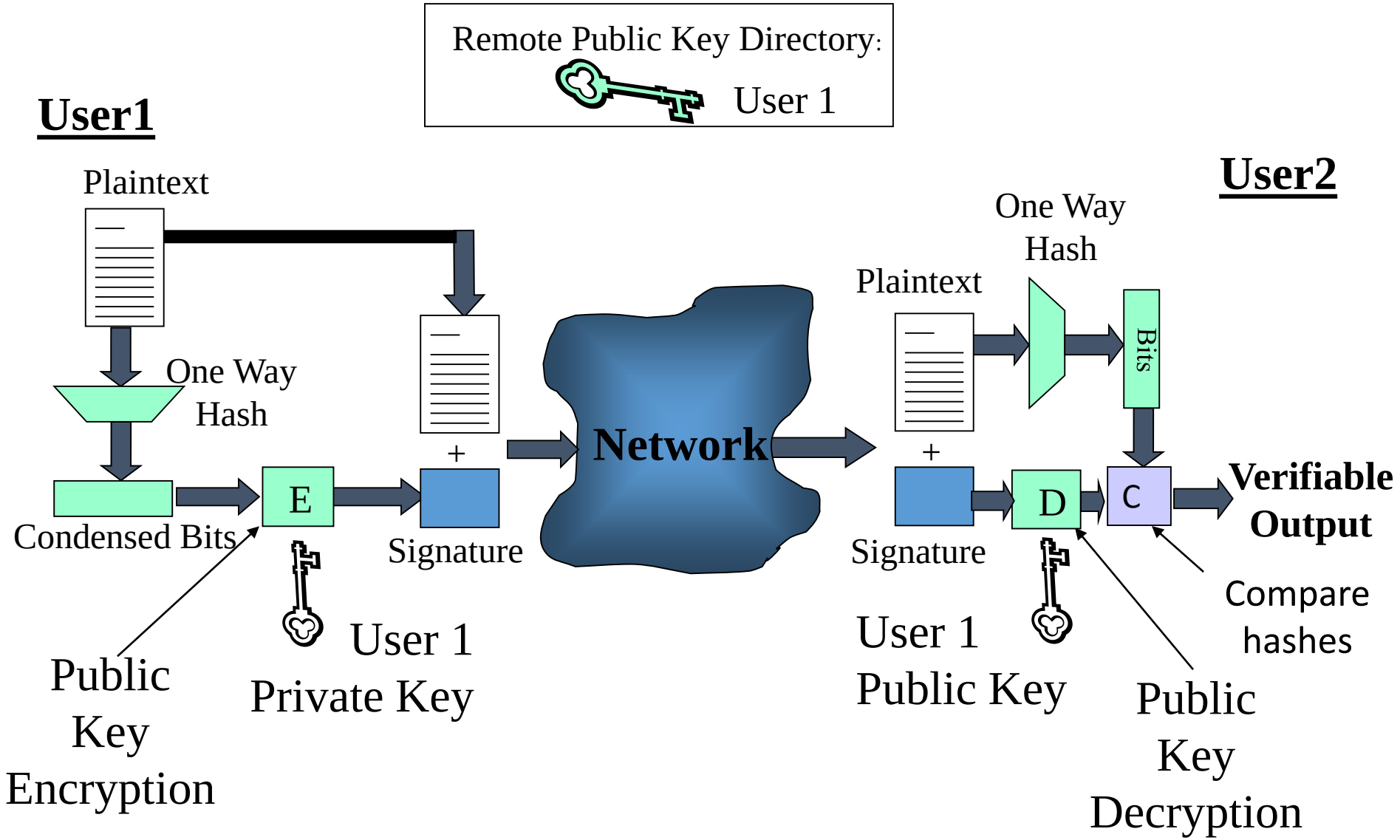
Research Subjects Needed

- A fellow graduate student needs subjects for an experiment on alternate password systems
- Participation requires:
  - two surveys which take about 4 minutes
  - reading a tutorial
  - logging into a system once a day for 9 days
- Participants will receive a **Starbucks Gift Card** for completing this study
- Email gridauthexperiment@gmail.com if you are interested

Digital Signature Process

- A hash of the data is created. The name of the sender is appended to the hash.
- The hash is encrypted with the private key of the sender
- The hash is appended to the data and transmitted together
- The receiver decrypts the hash with the public key of the sender
- The receiver calculates a hash of the message and compares it to the received hash

Digital Signature



Digital Signature Use

- Digitally signed email verifies the sender
- Signed applets or programs come from a known source and have not been modified
- Digitally signed programs cannot be modified or infected with a virus without detection
- Digitally signed documents cannot be changed without detection

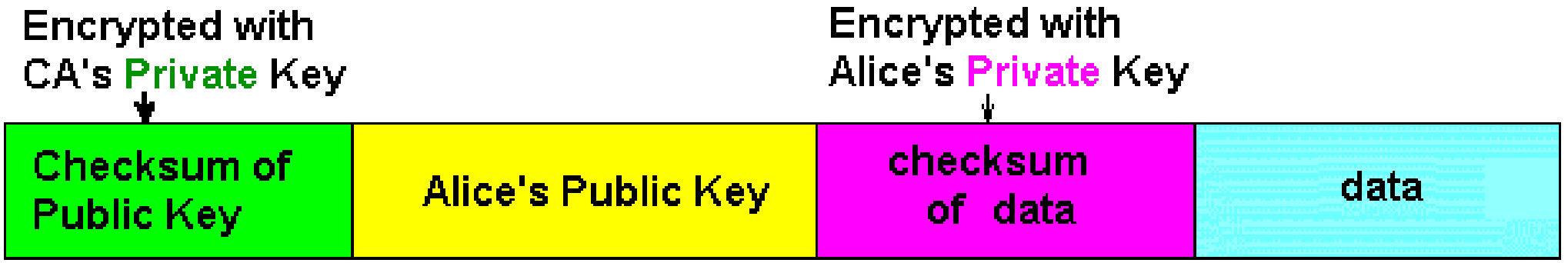
Signed Programs

- Many programs that are available on the web are digitally signed so the users can have some sense of trust to run them
- A program with an invalid signature should be treated with great caution

Digital Certificates

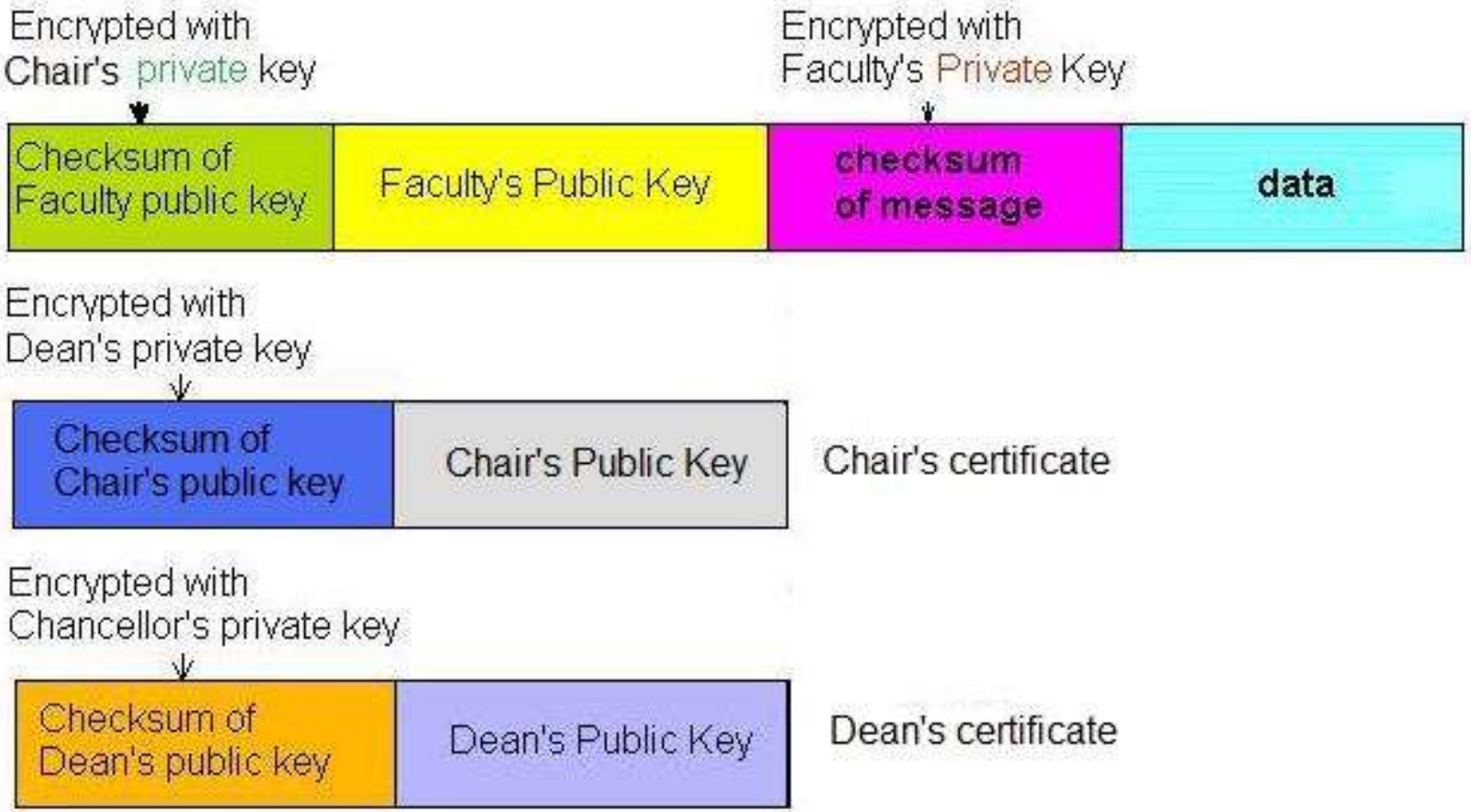
- A digital certificate contains a user's public key along with some information about the user, such as their email address
- The digital certificate is digitally signed by a Certificate Authority
- Certificate Authorities are venders of digital certificates
- Clients must know the public key of the Certificate Authority

Digital Certificates



University Certificates

- A chain of trust can be established from a single point in an organization.
- Only the top public key is needed by everyone



Digital Certificates contain

A. Private key of the owner
B. Public key of the owner
C. Public key of the CA
D. Hash of the CA key

X.509

- X.509 is a standard that defines the format of public key certificates defined by the International Telecommunications Union's Standardization sector (ITU-T)
- Used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS

Buying Digital Certificates

- Several companies sell digital certificates
- They are usually expensive for servers
- Free certificates are available for personal email

Creating Digital Certificates

- Security tools available with Java SDK

Tool Name	Brief Description
keytool	Manage keystores and certificates.
jarsigner	Generate and verify JAR signatures
policytool	GUI tool for managing policy files

Sign Something

- Acquire a digital certificate
- Send me a digitally signed email

or

- Sign a Jar file and email it to me
- Your name must be associated with the certificate
- Due by midnight on Tuesday, September 4

Certificate Revocation

- There are multiple reasons why you may wish to prevent the further use of a certificate
  - The key protecting the certificate has been compromised
  - The Certificate Authority has been compromised
  - The entity no longer belongs to the organization
  - The certificate was issued to an incorrect organization
  - The privilege to use the certificates has been withdrawn

Revocation Lists

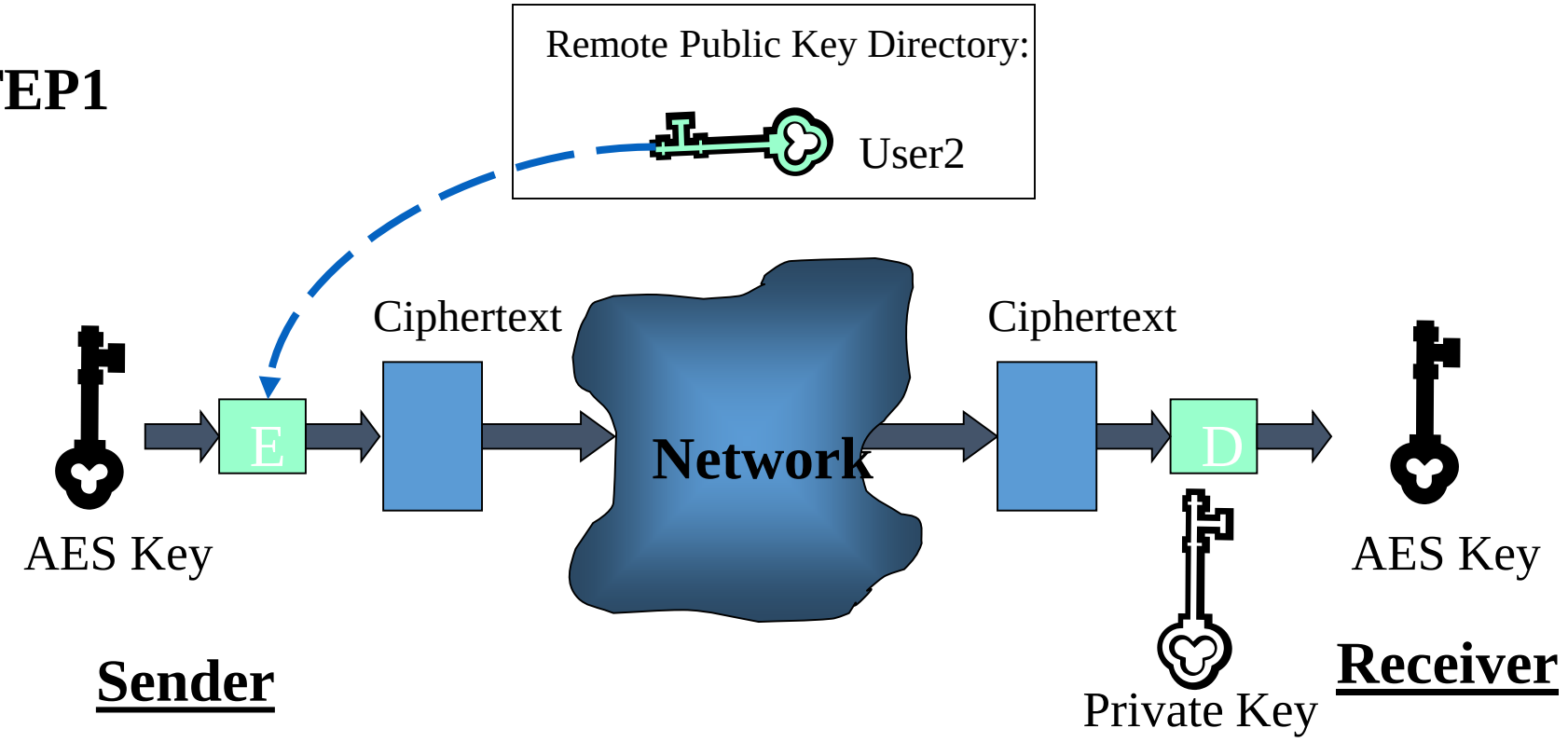
- Certificate Authorities keep a revocation list of the certificates they have issued that should not longer be used or accepted
- This does not include certificates that have passed their expiration date
- Any software that accepts a digital certificate from another entity should check the revocation list to see if it is still valid
  - Checking is not mandatory

Potential Revocation List Issues

- Contacting the Certificate Authority server is another step in establishing a connection
- It is another step the programmer has to take when coding the use of certificates and some skip it
- The CA could be subject to a denial of service attack

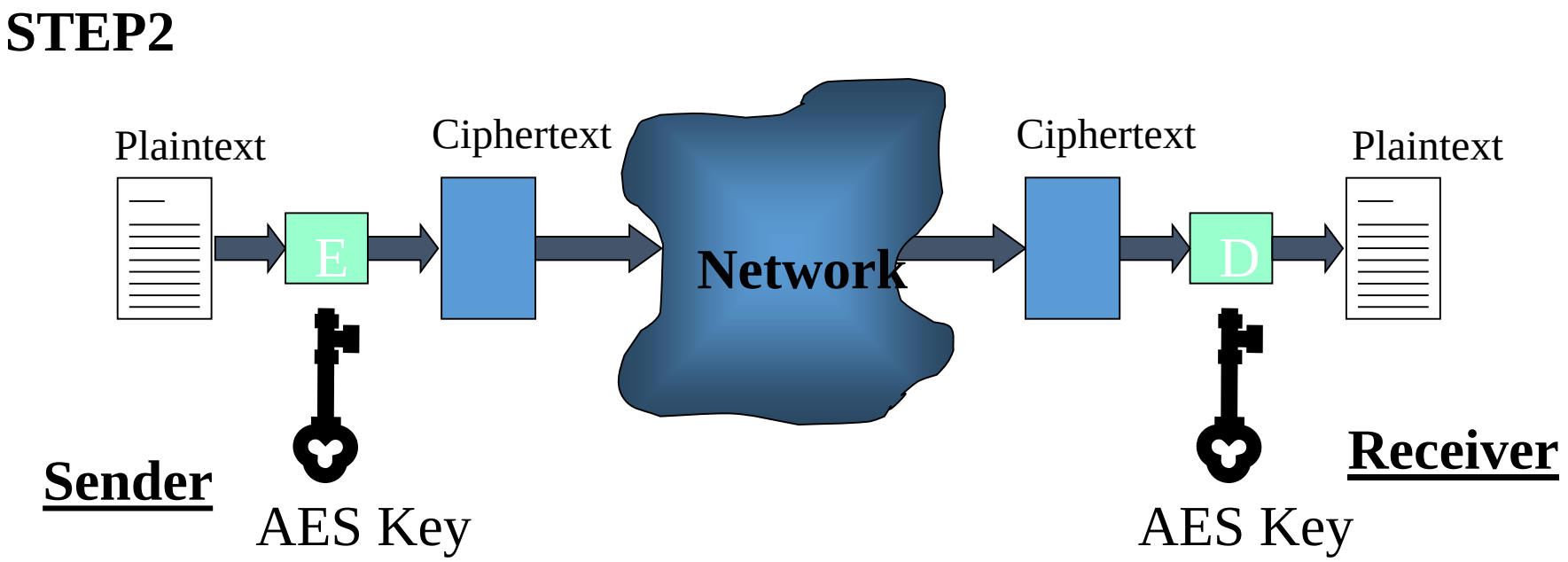
Hybrid Cryptography Overview (STEP 1)

- AES key is encrypted with public key cryptography using Public Key of receiver
- AES key sent to receiver
- Both users end up with a shared AES key



Hybrid Cryptography Overview (STEP 2)

- All following messages are encrypted with the AES key
- AES key is discarded after the session



SSL / TSL

- Hybrid encryption is used in the Secure Socket Layer (SSL) and Transport Layer Security (TLS)
- Used in HTTPS and other systems
- The identity of the communicating parties can be authenticated using public-key cryptography
- Typically only the server is authenticated

To authenticate, a client must send the server

A. Its AES key
B. Its IP address
C. Its Digital Certificate
D. Server’s public key
E. Hash of server’s key

Proxy Servers

- A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers
- Some proxy servers are intended for security testing and will allow the user to view and modify messages going between a user and the server
- A proxy server can establish an HTTPS connection to a server, but the user connection to the proxy may be flagged as invalid (the user can usually override this)

Who are you?

- **Authentication** is the process of verifying that the user or system is who they claim to be
- A system may be acting on behalf of a given principal

- Authentication differs from **authorization** which is the process of verifying that an authenticated subject has the authority to perform a given action

Enter userid and password

- Most systems use simple authentication
- The first step is called identification. You announce who you are
- The second step is called authentication. You prove that you are who you claim to be

Problems with Passwords

- Authentication by password is widely accepted and easy to implement
- Managing password security can be quite expensive; obtaining a valid password is a common way of gaining unauthorised access to a computer system
- Typical issues that need to be addressed:
  - how to get the password to the user
  - forgotten passwords
  - password guessing
  - password spoofing
  - compromise of the password file

Guessing Passwords

- **Exhaustive search** (brute force): Try all possible combinations of valid symbols up to a certain length.
- **Dictionary attack** tries all passwords from an on-line dictionary.
- You cannot prevent an attacker from accidentally guessing a valid password, but you can try to reduce the probability of a password compromise.

Popular Passwords

- The most popular passwords account for about 10% of all passwords used with 123456 representing about 3% of all passwords
- The top 10 all numerical PINs represent about 50% of all PINs used.

1. 123456
2. Password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou

Replay Threats

- Someone may be able to copy the data you send to a server to log in
- Even if they cannot decrypt the data, they might be able to send it to the server themselves to log in.
- This can be prevented by using different encryption keys for each login session or by using secure authentication protocols.

Augmenting password logins

- Some sites display a personalized phrase when you are asked to enter your password
- If you do not see the correct phrase, you should not enter your password
- The sites IP address can be used as part of the user authentication

Protecting the Password File

- The operating system maintains a file with user names and passwords
- An attacker could try to compromise the confidentiality or integrity of this password file
- Separate security relevant data from data that should be openly available.
  - In Unix, **`/etc/passwd`** contains both types of data

Storing the Password

- Instead of storing the password, many systems store the result of a one way function or hash of the password, such as SHA-1
- When a user enters a password, it is hashed and compared with the stored hash value
- If someone gets access to the password file, they still do not know the passwords

If an attacker has a list of passwords, they can determine the password from a list of hashed passwords.

A. True
B. False
C. All of the above
D. None of the above

Means of Authentication

- What you know
- What you have
- Where you are
- What you are
- What you can do

What You Have

- Users can be required to have a device to identify them
  - ID card
  - smartcard
  - USB with security file
- Should be used in conjunction with other authentication methods

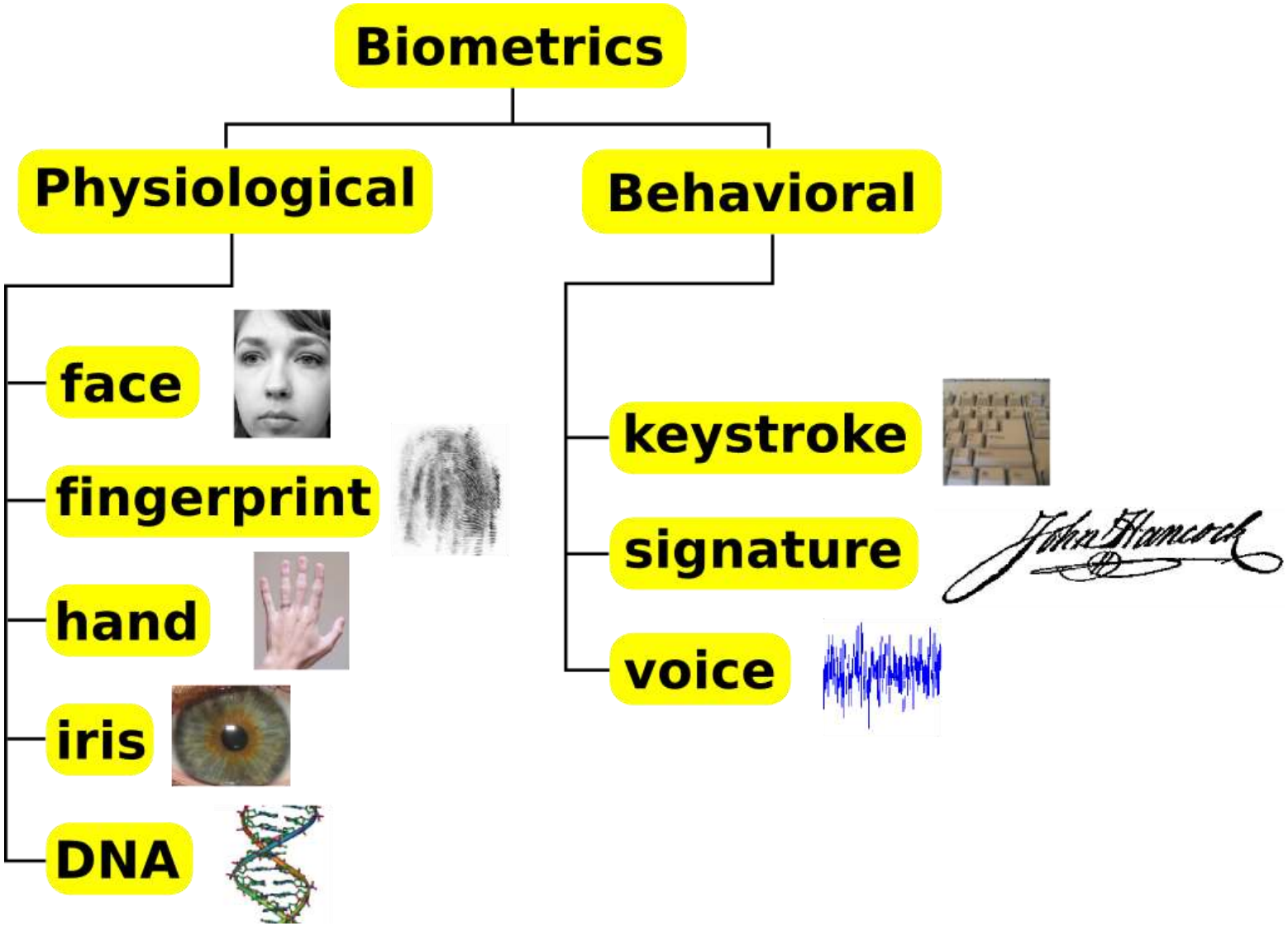
Where You Are

- Some operating systems grant access only if you log on from a certain terminal
  - Typically the IP address of the computer is used
- Global Positioning System (GPS) might be used to established the precise geographical location of a user during authentication

What You Can Do

- People perform mechanical tasks in a way that is both repeatable and specific to the individual
- Users could sign on a special pad that measures attributes like writing speed and writing pressure
- On a keyboard, typing speed and key strokes intervals can be used to authenticate individual users

What You Are - Biometrics



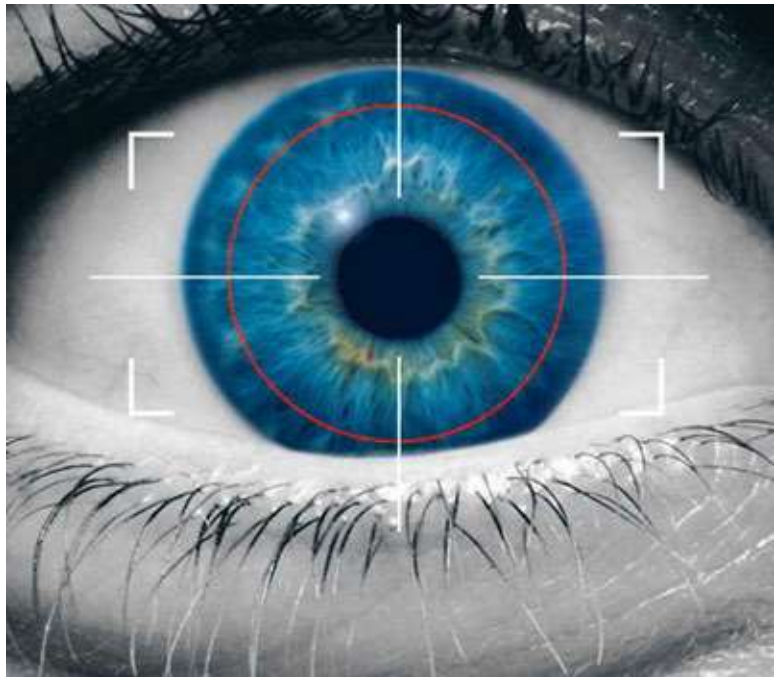
Fingerprints

- Fingerprint readers are simple and inexpensive
- For most people they have high reliability
- Not every person has usable fingerprints

Your finger doesn’t have to be attached to your hand

Iris Matching

- Every person’s iris is said to be unique
- You have to get a close image
- Better for authentication than recognition



Revoking Biometrics

- You can easily change your password if someone learns what it is
- How do you change your fingerprint (or other biometric) if someone gets a copy?

- What if the biometric is unavailable?

Research Subjects Needed

- A fellow graduate student needs subjects for an experiment on alternate password systems
- Participation requires:
  - two surveys which take about 4 minutes
  - reading a tutorial
  - logging into a system once a day for 9 days
- Participants will receive a **Starbucks Gift Card** for completing this study
- Email gridauthexperiment@gmail.com if you are interested

Programming Assignment

- The programming assignment to encrypt and decrypt a file is due before midnight on Thursday, August 30
- Upload your source code to Blackboard along with a short explanation of the algorithm used and the format of the file
- This is a team project to be done by pairs of students