Cryptography

Secure Communication

Needs and Requirements

- Well established needs for secure communication
  - War time communication
  - Business transactions
  - Illicit Love Affairs
- Requirements of secure communication
  1. Secrecy
     - Only intended receiver understands the message
  2. Authentication
     - Sender and receiver need to confirm each others identity
  3. Message Integrity
     - Ensure that their communication has not been altered, either maliciously or by accident during

Cryptography

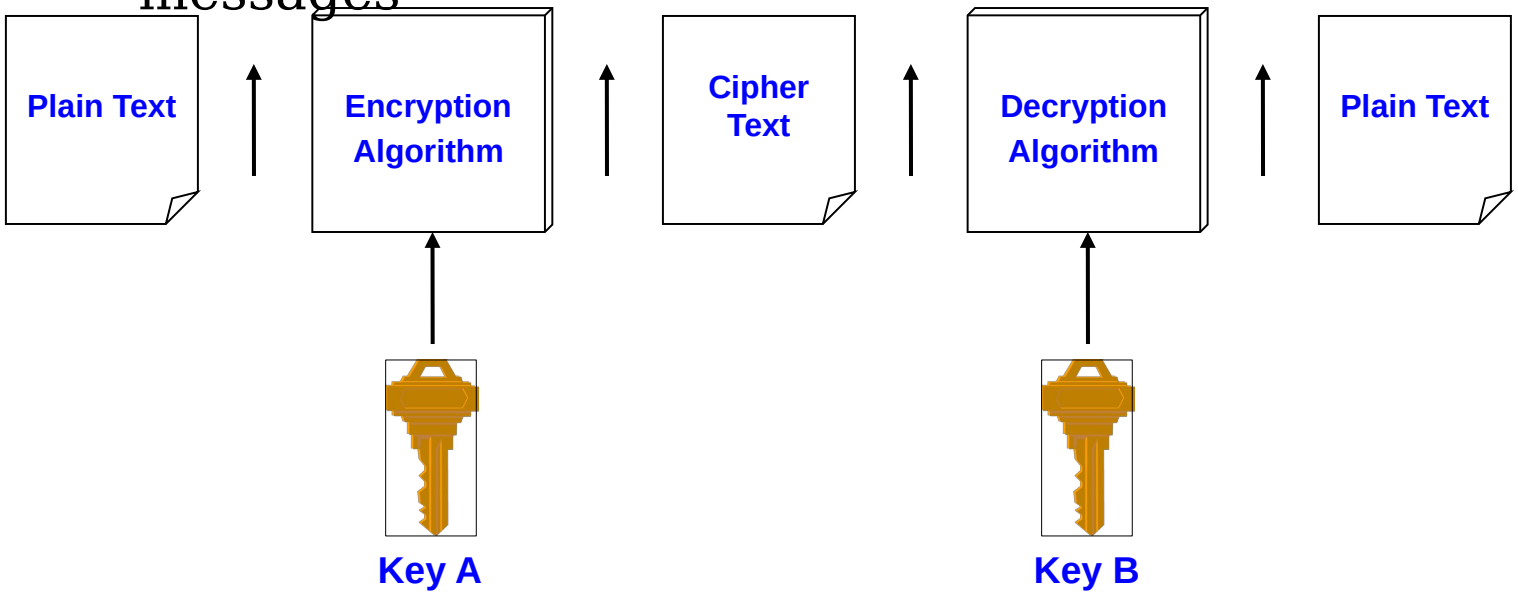
Basics

- Cryptography is the science of secret, or hidden writing
- It has two main Components:
  1. Encryption
     - Practice of hiding messages so that they can not be read by anyone other than the intended recipient
  2. Authentication & Integrity
     - Ensuring that users of data/resources are the persons they claim to be and that a message has not been surreptitiously altered

Encryption

Cipher

- Cipher is a method or algorithm for the encrypting messages



- Encryption algorithms are standardized & published
- The key which is an input to the algorithm is secret
  - Key is a string of numbers or characters
  - If same key is used for encryption & decryption the algorithm is called symmetric
  - If different keys are used for encryption & decryption the algorithm is called asymmetric

Encryption

Symmetric Algorithms*

- Algorithms in which the key for encryption and decryption are the same are Symmetric
  - Example: Caesar Cipher
- Types:
  1. Block Ciphers
     - Encrypt data one block at a time (typically 64 bits, or 128 bits)
     - Used for a single message
  2. Stream Ciphers
     - Encrypt data one bit or one byte at a time
     - Used if data is a constant stream of information

Symmetric Encryption

Key Strength

- Strength of algorithm is determined by the size of the key
  - The longer the key the more difficult it is to crack
- Key length is expressed in bits
  - Typical key sizes vary between 48 bits and 448 bits
- Set of possible keys for a cipher is called key space
  - For 40-bit key there are 2^{40} possible keys
  - For 128-bit key there are 2^{128} possible keys
  - Each additional bit added to the key length doubles the security
- To crack the key the hacker has to use brute-force

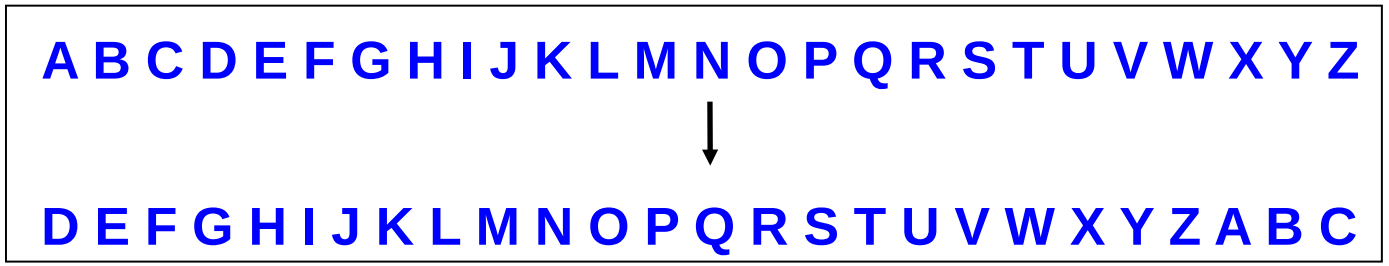
  (i.e. try all the possible keys till a key that works is found)

  Super Computer can crack a 56 bit key in 24 hours

Substitution Ciphers

Caesar Cipher*

- Caesar Cipher is a method in which each letter in the alphabet is rotated by three letters as shown

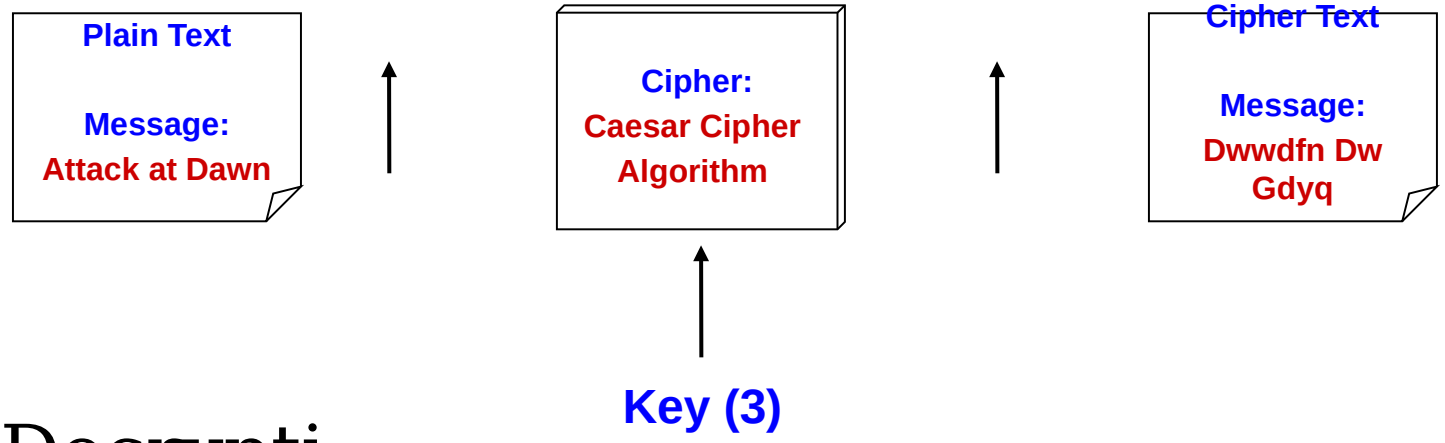


- Let us try to encrypt the message
  - Attack Dawn

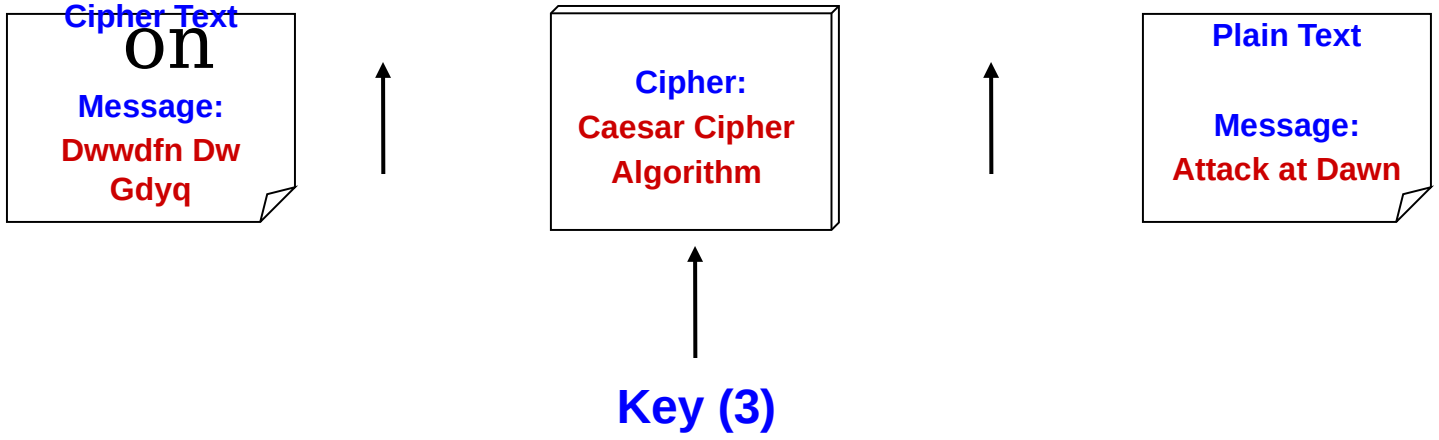
Substitution Ciphers

Caesar Cipher

Encryption



Decryption



How many different keys are possible?

Substitution Cipher

Monoalphabetic Cipher*

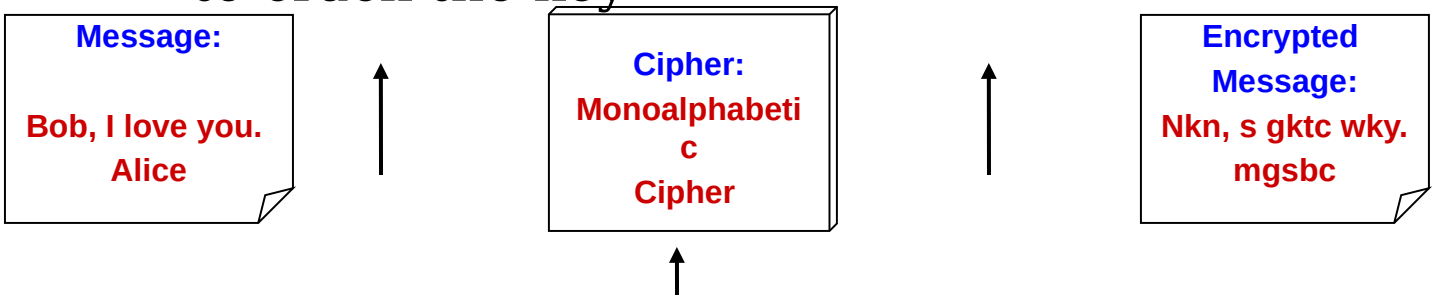
- Any letter can be substituted for any other letter
  - Each letter has to have a unique substitute

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

↓

M N B V C X Z A S D F G H J K L P O I U Y T R E W Q

- There are 26! pairing of letters (~10^{26})
- Brute Force approach would be too time consumin
  - Statistical Analysis(e occurs 13%) would make it feasible to crack the key



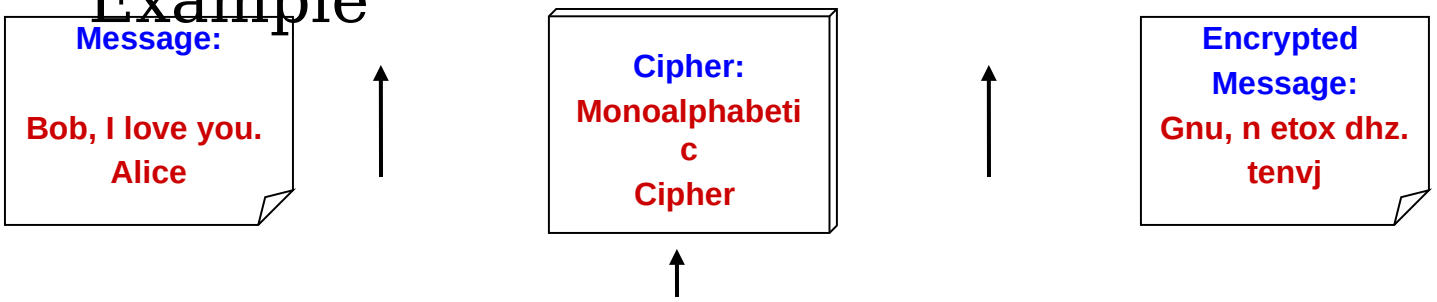
Substitution Cipher

Polyalphabetic Caesar Cipher*

- Developed by Blaise de Vigenere
  - Also called Vigenere cipher
- Uses a sequence of monoalpabetic ciphers in tandem
  - e.g. C_1, C_2, C_2, C_1, C_2

Plain Text	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
	↓
C1(k=6)	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
C2(k=20)	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S

- Example



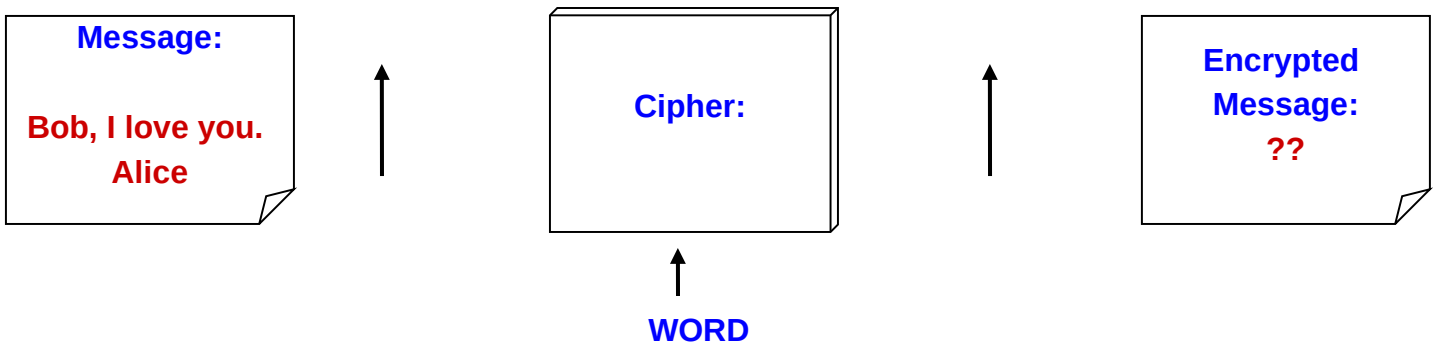
Substitution Cipher

Using a key to shift alphabet*

- Obtain a key to for the algorithm and then shift the alphabets
  - For instance if the key is word we will shift all the letters by four and remove the letters w, o, r, & d from the encryption
- We have to ensure that the mapping is one-to-one
  - no single letter in plain text can map to two different letters in cipher text
  - no single letter in cipher text can map to two different letters in plain text

Plain Text 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

C1(k=6) W O R D A B C E F G H I J K L M N P Q S T U V X Y Z



Transposition Cipher

Columnar Transposition*

- This involves rearrangement of characters on the plain text into columns
- The following example shows how letters are transformed
  - If the letters are not exact multiples of the transposition size there may be a few short letters in the last column which can be padded with an infrequent letter such as x or z.

Plain Text	Cipher Text
T H I S I	T S S O H
S A M E S	O A N I W
S A G E T	H A A S O
O S H O W	L R S T O
H O W A C	I M G H W
O L U M N	U T P I R
A R T R A	S E E O A
N S P O S	M R O O K
I T I O N	I S T W C
W O R K S	N A S N S

Ciphers

Shannon's Characteristics of "Good" Ciphers

- The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
- The set of keys and the enciphering algorithm should be free from complexity.
- The implementation of the process should be as simple as possible.
- Errors in ciphering should not propagate and cause corruption of further information in the message.
- The size of the enciphered text should

Encryption Systems

Properties of Trustworthy Systems

- It is based on sound mathematics.
  - Good cryptographic algorithms are are derived from solid principles.
- It has been analyzed by competent experts and found to be sound.
  - Since it is hard for the writer to envisage all possible attacks on the algorithm
- It has stood the “test of time.”
  - Over time people continue to review both mathematical foundations of an algorithm and the way it builds upon those foundations.
  - The flaws in most algorithms are discovered soon after their release.

Data Encryption Standard (DES)

Basics*

- Goal of DES is to completely scramble the data and key so that every bit of cipher text depends on every bit of data and ever bit of key
- DES is a block Cipher Algorithm
  - Encodes plaintext in 64 bit chunks
  - One parity bit for each of the 8 bytes thus it reduces to 56 bits
- It is the most used algorithm
  - Standard approved by US National Bureau of Standards for Commercial and nonclassified US government use in 1993

Encryption Algorithm

Summary

Algorithm	Type	Key Size	Features
DES	Block Cipher	56 bits	Most Common, Not strong enough
TripleDES	Block Cipher	168 bits (112 effective)	Modification of DES, Adequate Security
Blowfish	Block Cipher	Variable (Up to 448 bits)	Excellent Security
AES	Block Cipher	Variable (128, 192, or 256 bits)	Replacement for DES, Excellent Security
RC4	Stream Cipher	Variable (40 or 128 bits)	Fast Stream Cipher, Used in most SSL implementations

Symmetric Encryption

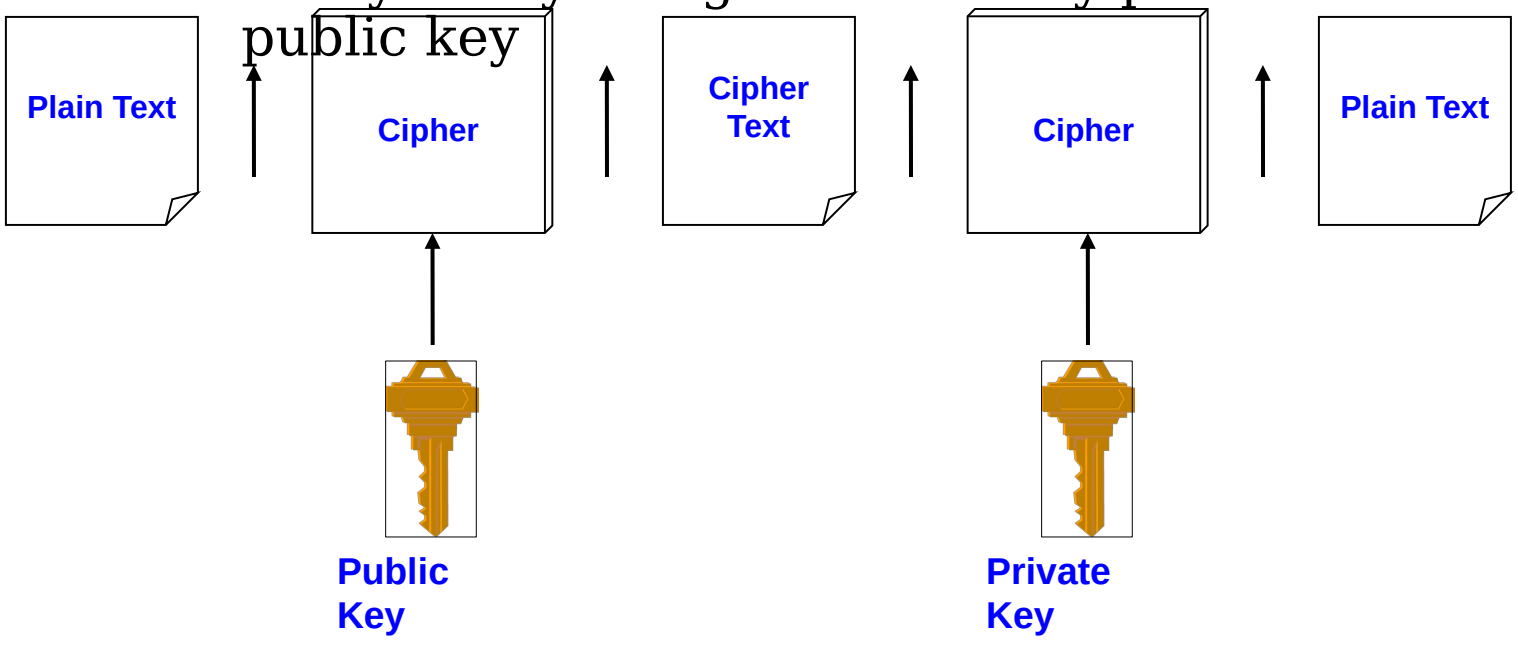
Limitations

- Any exposure to the secret key compromises secrecy of ciphertext
- A key needs to be delivered to the recipient of the coded message for it to be deciphered
  - Potential for eavesdropping attack during transmission of key

Asymmetric Encryption

Basics*

- Uses a pair of keys for encryption
  - Public key for encryption
  - Private key for decryption
- Messages encoded using public key can only be decoded by the private key
  - Secret transmission of key for decryption is not required
  - Every entity can generate a key pair and release its public key



Asymmetric Encryption

Types

- Two most popular algorithms are RSA & El Gamal
  - RSA
    - Developed by Ron Rivest, Adi Shamir, Len Adelman
    - Both public and private key are interchangable
    - Variable Key Size (512, 1024, or 2048 buts)
    - Most popular public key algorithm
  - El Gamal
    - Developed by Taher ElGamal
    - Variable key size (512 or 1024 bits)
    - Less common than RSA, used in protocols like PGP

Asymmetric Encryption

RSA

- Choose two large prime numbers p & q
- Compute n=pq and z=(p-1)(q-1)
- Choose number e, less than n, which has no common factor (other than 1) with z
- Find number d, such that ed – 1 is exactly divisible by z
- Keys are generated using n, d, e
  - Public key is (n,e)
  - Private key is (n, d)
- Encryption: $c = m^e \bmod n$
  - m is plain text
  - c is cipher text
- Decryption: $m = c^d \bmod n$
- Public key is shared and the private key is hidden

Asymmetric Encryption

RSA

- P=5 & q=7
- n=5*7=35 and z=(4)*(6) = 24
- e = 5
- d = 29 , (29x5 –1) is exactly divisible by 24, 6 times of 24
- Keys generated are
  - Public key: (35,5)
  - Private key is (35, 29)
- Encrypt the word love using ($c = m^e \bmod n$)
  - Assume that the alphabets are between 1 & 26, 1 for a, e=5

Plain Text	Numeric Representation	m^e	Cipher Text ($c = m^e \bmod n$)
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

Asymmetric Encryption

RSA

- Decrypt the word love using ($m = c^d \bmod n$)
  - n = 35, c=29

Cipher Text	c^d	($m = m^e \bmod n$)	Plain Text
17	481968572106750915091411825223072000	17	l
15	127834039488589391112327575683594 00	15	o
22	852643319086537701956194499721110000000	22	v
10	10000000000000000000000000000	10	e

Asymmetric Encryption

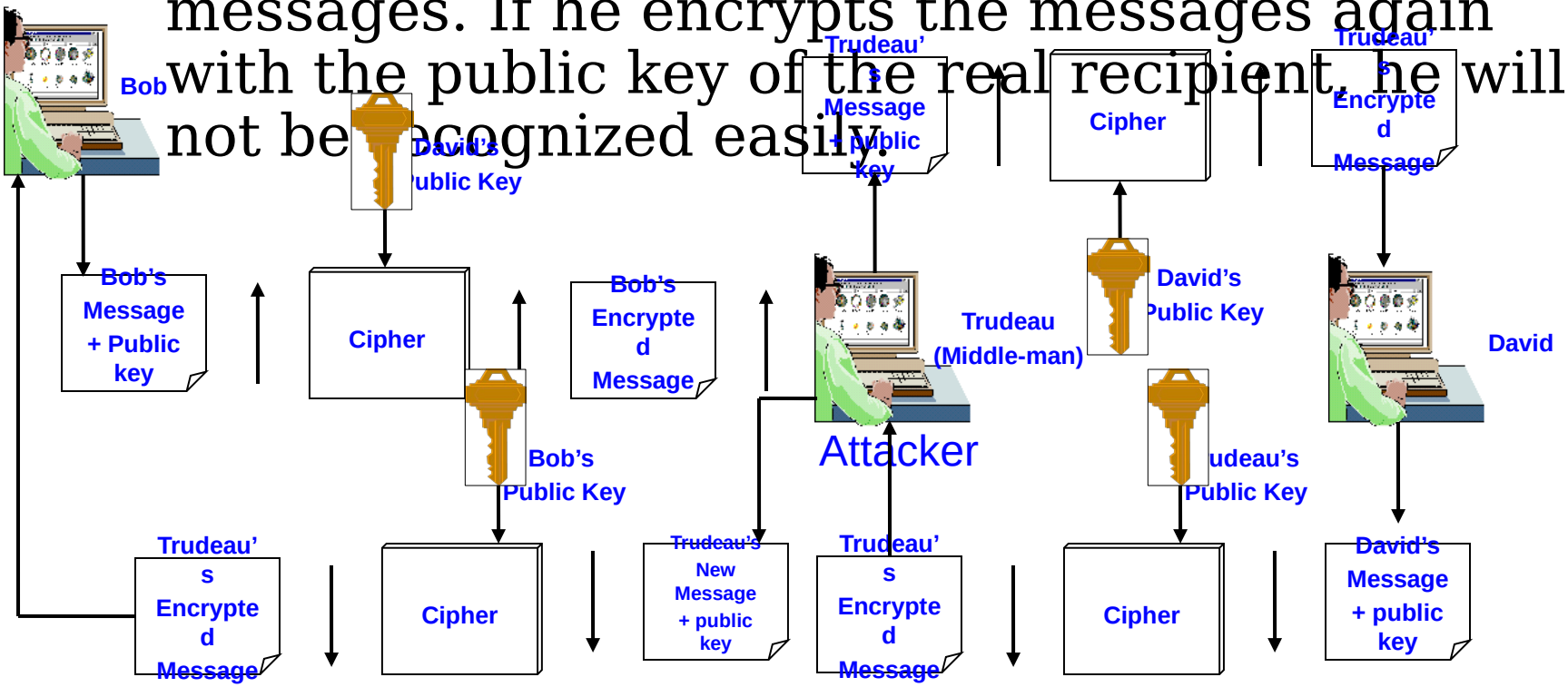
Weaknesses

- Efficiency is lower than Symmetric Algorithms
  - A 1024-bit asymmetric key is equivalent to 128-bit symmetric key
- Potential for man-in-the middle attack
- It is problematic to get the key pair generated for the encryption

Asymmetric Encryption

Man-in-the-middle Attack

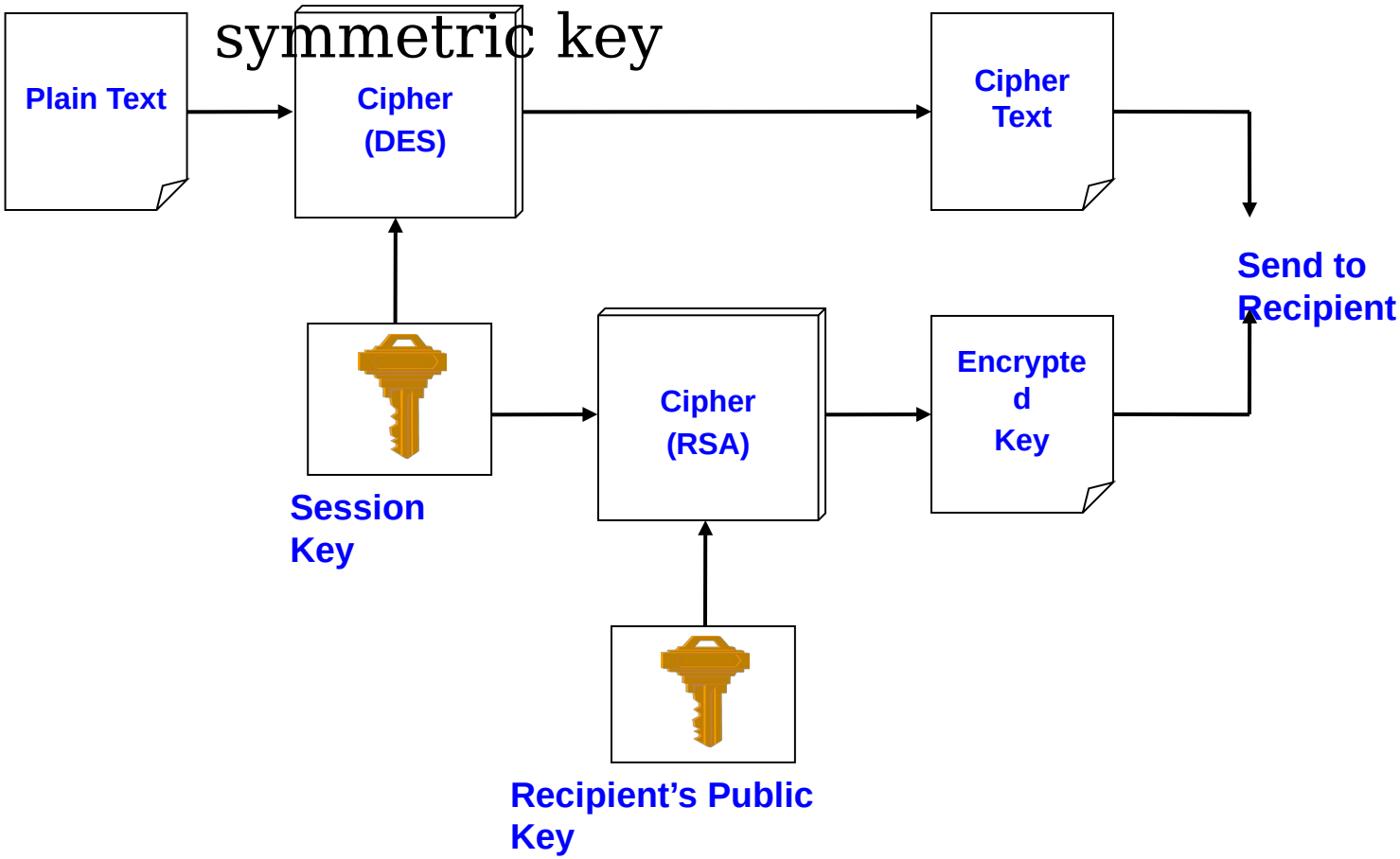
- Hacker could generate a key pair, give the public key away and tell everybody, that it belongs to somebody else. Now, everyone believing it will use this key for encryption, resulting in the hacker being able to read the messages. If he encrypts the messages again with the public key of the real recipient, he will not be recognized easily.



Asymmetric Encryption

Session-Key Encryption*

- Used to improve efficiency
  - Symmetric key is used for encrypting data
  - Asymmetric key is used for encrypting the symmetric key



Asymmetric Encryption

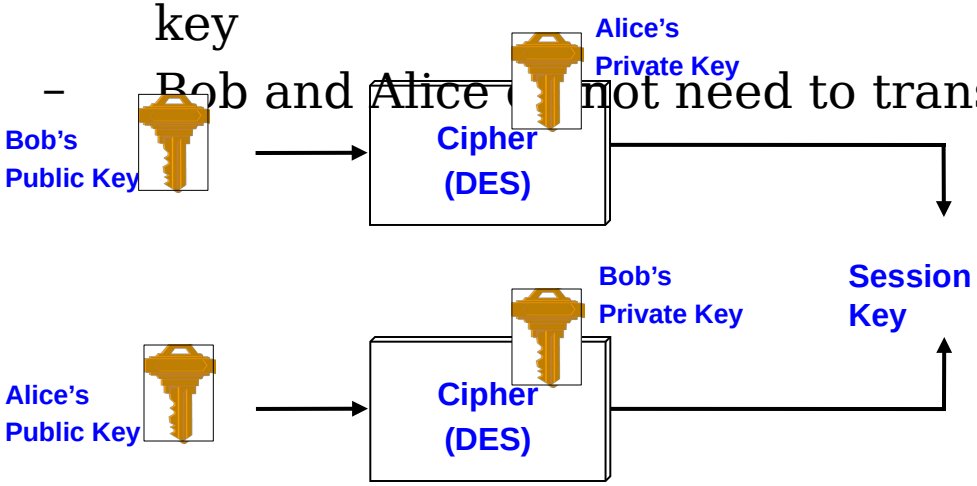
Encryption Protocols

- Pretty Good Privacy (PGP)
  - Used to encrypt e-mail using session key encryption
  - Combines RSA, TripleDES, and other algorithms
- Secure/Multipurpose Internet Mail Extension (S/MIME)
  - Newer algorithm for securing e-mail
  - Backed by Microsoft, RSA, AOL
- Secure Socket Layer(SSL) and Transport Layer Socket(TLS)
  - Used for securing TCP/IP Traffic
  - Mainly designed for web use
  - Can be used for any kind of internet traffic

Asymmetric Encryption

Key Agreement

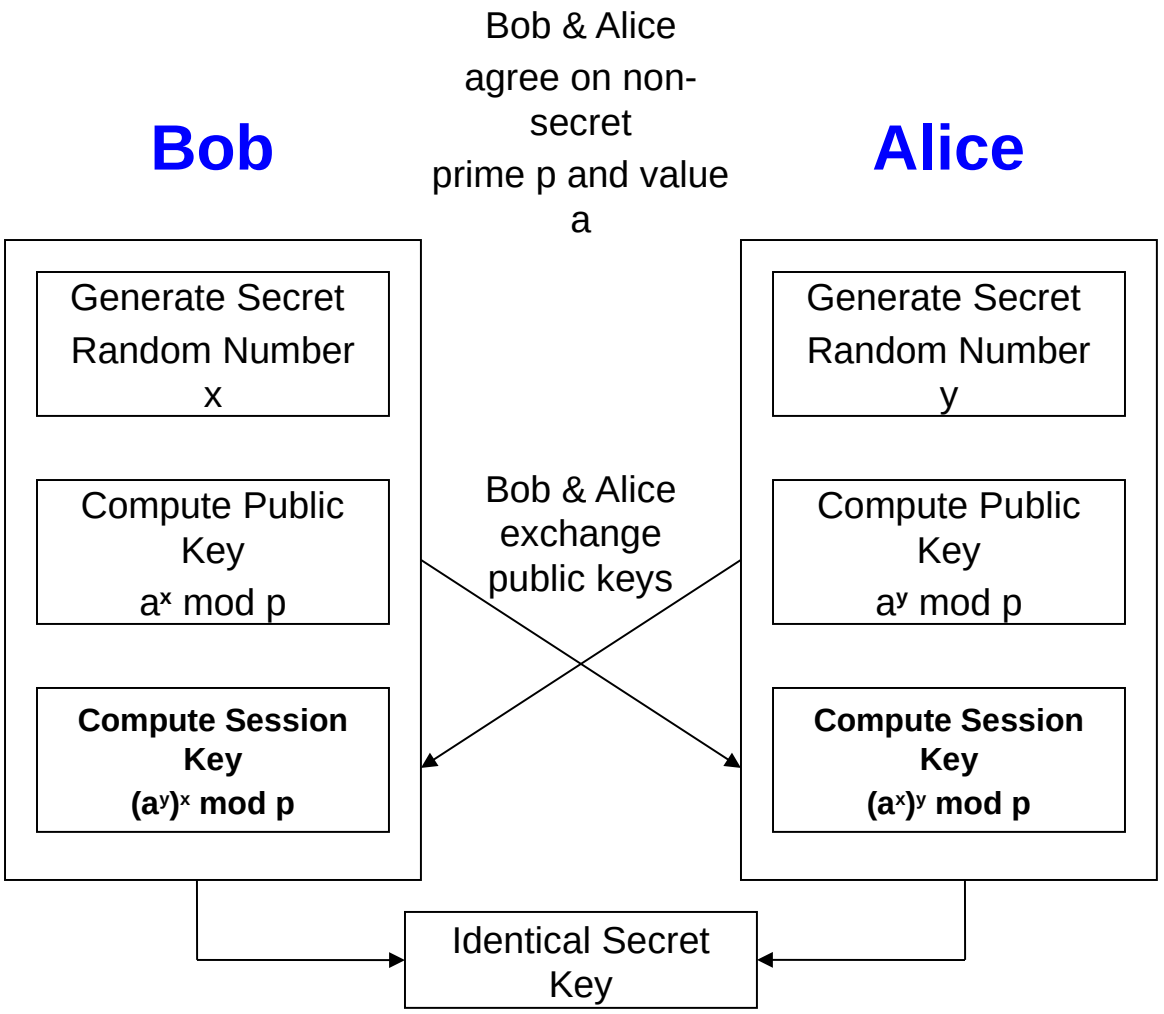
- Key agreement is a method to create secret key by exchanging only public keys.
- Example
  - Bob sends Alice his public key
  - Alice sends Bob her public key
  - Bob uses Alice's public key and his private key to generate a session key
  - Alice uses Bob's public key and her private key to generate a session key
  - Using a key agreement algorithm both will generate same key
  - Bob and Alice do not need to transfer any key



Alice and Bob Generate Same Session Key!

Asymmetric Encryption

Key Diffie-Hellman Mathematical Analysis*



Asymmetric Encryption

Key Agreement con't.

- Diffie-Hellman is the first key agreement algorithm
  - Invented by Whitfield Diffie & Martin Hellman
  - Provided ability for messages to be exchanged securely without having to have shared some secret information previously
  - Inception of public key cryptography which allowed keys to be exchanged in the open
- No exchange of secret keys
  - Man-in-the middle attack avoided

Authentication

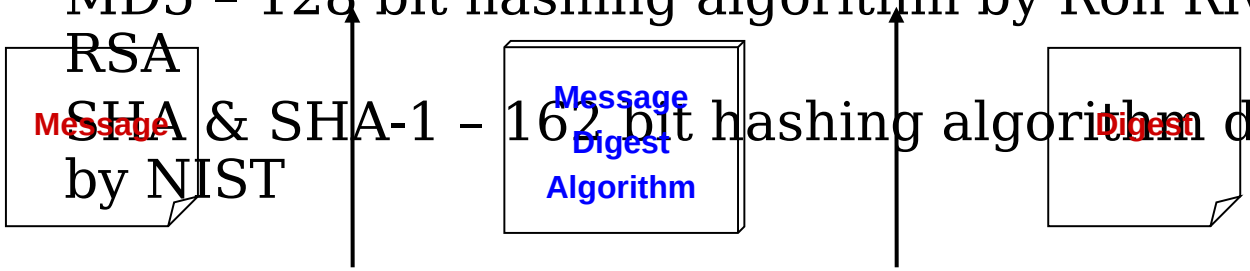
Basics

- Authentication is the process of validating the identity of a user or the integrity of a piece of data.
- There are three technologies that provide authentication
  - Message Digests / Message Authentication Codes
  - Digital Signatures
  - Public Key Infrastructure
- There are two types of user authentication:
  - Identity presented by a remote or application participating in a session

Authentication

Message Digests

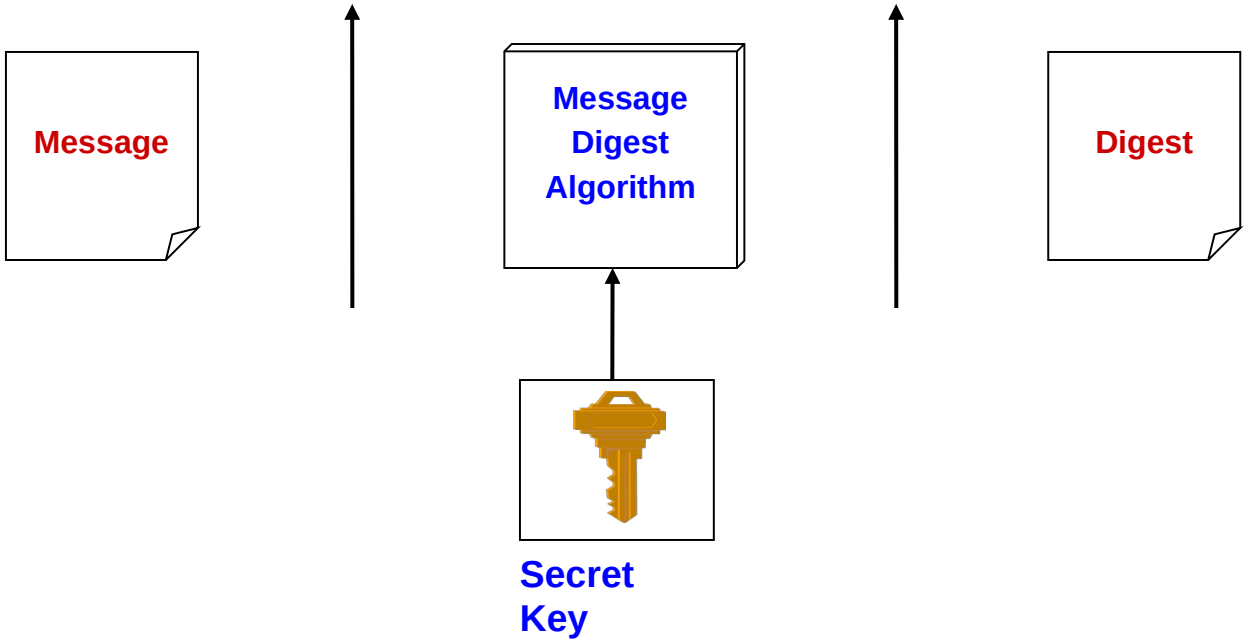
- A message digest is a fingerprint for a document
- Purpose of the message digest is to provide proof that data has not altered
- Process of generating a message digest from data is called hashing
- Hash functions are one way functions with following properties
  - Infeasible to reverse the function
  - Infeasible to construct two messages which hash to same digest
- Commonly used hash algorithms are
  - MD5 – 128 bit hashing algorithm by Ron Rivest of RSA
  - SHA & SHA-1 – 162 bit hashing algorithm developed by NIST



Message Authentication Codes

Basics

- A message digest created with a key
- Creates security by requiring a secret key to be possesses by both parties in order to retrieve the message



Password Authentication

Basics*

- Password is secret character string only known to user and server
- Message Digests commonly used for password authentication
- Stored hash of the password is a lesser risk
  - Hacker can not reverse the hash except by brute force attack
- Problems with password based authentication
  - Attacker learns password by social engineering
  - Attacker cracks password by brute-force and/or guesswork
  - Eavesdrops password if it is communicated unprotected over the network
  - Replays an encrypted password back to the authentication server

Authentication Protocols

Basics

- Set of rules that governs the communication of data related to authentication between the server and the user
- Techniques used to build a protocol are
  - Transformed password
    - Password transformed using one way function before transmission
    - Prevents eavesdropping but not replay
  - Challenge-response
    - Server sends a random value (challenge) to the client along with the authentication request. This must be included in the response
    - Protects against replay
  - Time Stamp
    - The authentication from the client to server must have time-stamp embedded
    - Server checks if the time is reasonable
    - Protects against replay
    - Depends on synchronization of clocks on computers
  - One-time password
    - New password obtained by passing user-password through one-way function n times which keeps incrementing
    - Protects against replay as well as eavesdropping

Authentication Protocols

Kerberos

- Kerberos is an authentication service that uses symmetric key encryption and a key distribution center.
- Kerberos Authentication server contains symmetric keys of all users and also contains information on which user has access privilege to which services on the network

Authentication

Personal Tokens

- Personal Tokens are hardware devices that generate unique strings that are usually used in conjunction with passwords for authentication
- Different types of tokens exist
  - Storage Token: A secret value that is stored on a token and is available after the token has been unlocked using a PIN
  - Synchronous one-time password generator: Generate a new password periodically (e.g. each minute) based on time and a secret code stored in the token
  - Challenge-response: Token computes a number based on a challenge value sent by the server
  - Digital Signature Token: Contains the digital signature private key and computes a computes a digital signature on a supplied data value
- A variety of different physical forms of tokens

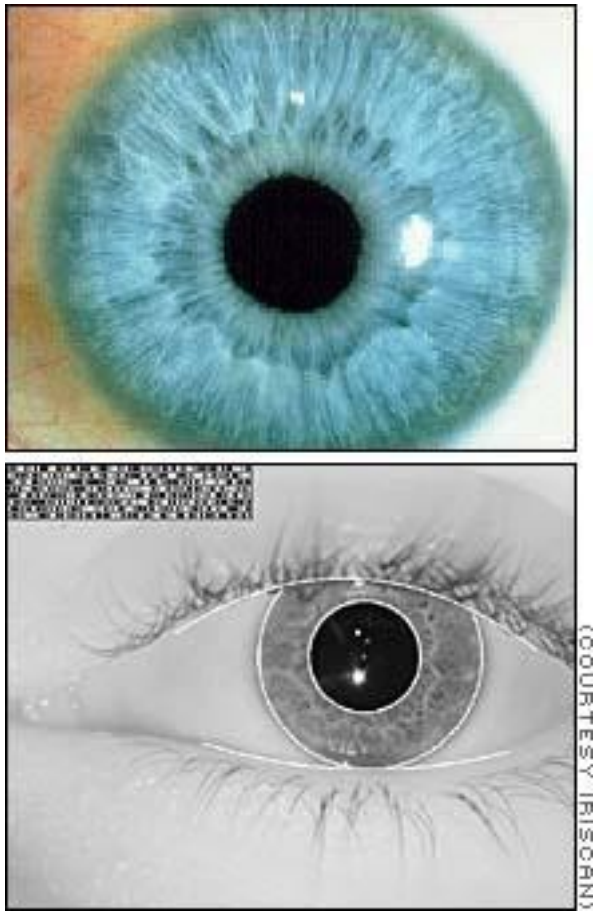
Authentication

Biometrics

- Uses certain biological characteristics for authentication
  - Biometric reader measures physiological indicia and compares them to specified values
  - It is not capable of securing information over the network
- Different techniques exist
  - Fingerprint Recognition
  - Voice Recognition
  - Handwriting Recognition
  - Face Recognition
  - Retinal Scan
  - Hand Geometry Recognition

Authentication

Iris Recognition



The scanning process takes advantage of the natural patterns in people's irises, digitizing them for identification purposes

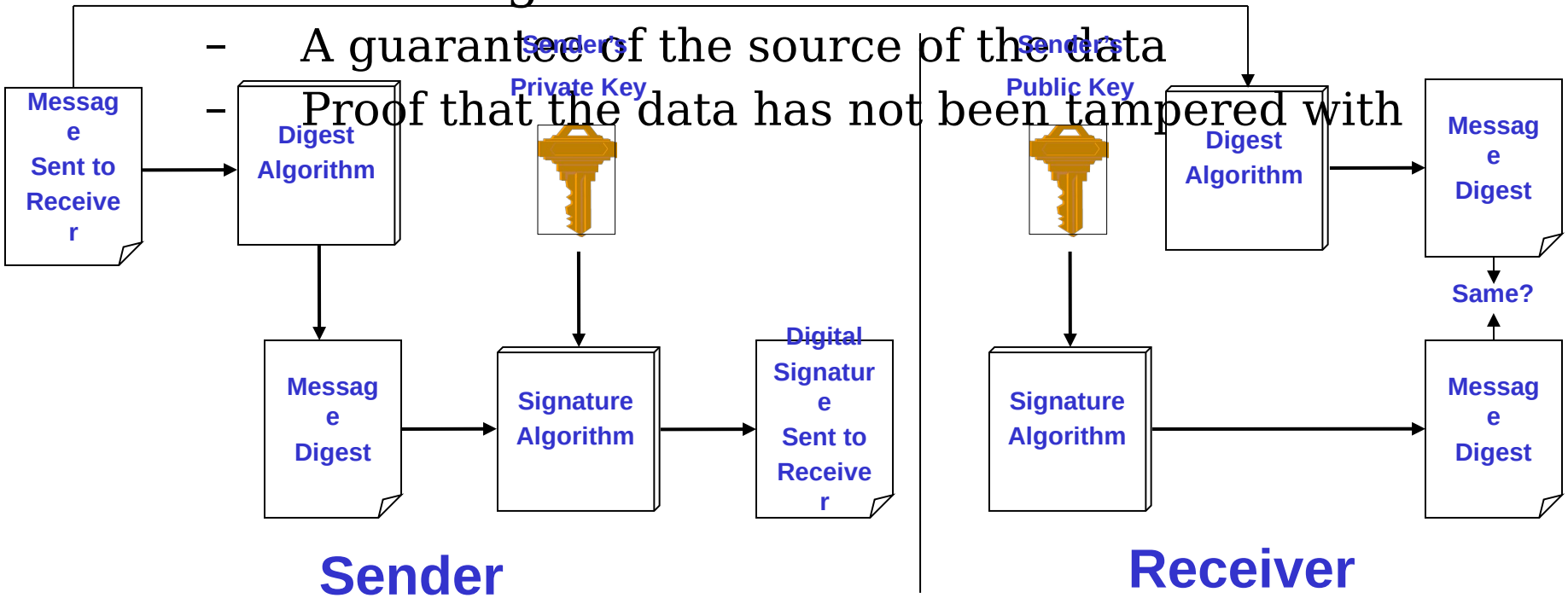
Facts

- Probability of two irises producing exactly the same code: 1 in 10 to the 78th power
- Independent variables (degrees of freedom) extracted: 266
- IrisCode record size: 512 bytes
- Operating systems compatibility: DOS and Windows (NT/95)
- Average identification speed (database of 100,000 IrisCode records): one to two seconds

Authentication

Digital Signatures*

- A digital signature is a data item which accompanies or is logically associated with a digitally encoded message.
- Type – Standard, Basic, and Advanced & Qualified
- It has two goals
  - A guarantee of the source of the data
  - Proof that the data has not been tampered with



Authentication

Digital Signature Types

- Domain Validated (DV) Certificates: These certificates are issued based on the validation of the domain name only. They are typically issued quickly and at a low cost.
- Organization Validated (OV) Certificates: These certificates are issued after validating the organization's legal existence and address. They offer more assurance than DV certificates, but take longer to issue.
- Extended Validation (EV) Certificates: These certificates provide the highest level of assurance as they are issued after a thorough background check of the organization and its ownership. They are typically issued to businesses and take the

Authentication

Digital Signature Types (Continue)

- Wildcard Certificates: These certificates can be used to secure multiple subdomains of a domain using a single certificate.
- Multi-Domain (SAN) Certificates: These certificates can be used to secure multiple domain names using a single certificate.
- Self-Signed Certificates: These certificates are issued and signed by the same entity and are not verified by a third-party. They are typically used for testing and internal use.

Authentication

Digital Cerftificates

- A digital certificate is a signed statement by a trusted party that another party's public key belongs to them.
  - This allows one certificate authority to be authorized by a different authority (root CA)
- Top level certificate must be self signed
- Any one can start a certificate authority
  - Name recognition is key to some one recognizing a certificate authority
  - Verisign is industry standard certificate authority