Privacy, Security and Usability

Security and Cryptography

INTRODUCTION TO ENCRYPTION

Encryption

- What is encryption?
  - A tool that can help achieve security properties
- Main goal:
  - Encoding a message so that it can not be read by unauthorized entities

Motivation

- “The basics of asymmetric cryptography are fundamental concepts that any member of society who wants to understand how the world works, or could work, needs to understand. They are as fundamental as the basics of supply and demand and monetary inflation”

Phil Libin, Evernote

Encryption

- Two main encryption approaches:
  - Symmetric encryption: same key used for both encryption and decryption
  - Asymmetric encryption:
    - Uses a pair of keys: public and private
      - Public key disseminated widely
      - Private key only known to the owner

Cybersecurity and Encryption

- What could we encrypt?
  - Data on storage, such as hard drive, disks, USB stick
  - Outgoing emails
  - Text messages, SMS, etc.
  - Your web browsing activity
    - Search history, pages you visited, etc.

Why is encryption useful?

- Can be used for multiple functionality, such as:
  - Confidentiality – only authorized users will have the key to decrypt the message
  - Integrity – message can not be tampered with
  - Authentication – only holder of key can read or generate the message

Encryption and Usability

- Passwords/keys typically used in encryption
- Has to be secret
- Should be memorable
- Needs to be stored safely

Does encryption solve all issues?

- Additional cyber-security threats:
  - Malware
  - Web trackers
  - Phishing emails and links
  - Compromised certificate authority

CRYPTOGRAPHY

https://www.tripwire.com/state-of-security/security-data-protection/cryptography/ordinary-people-need-cryptography/

Encryption

- Encoding a message so that its meaning is not obvious

Problems Addressed by Encryption

- Suppose a sender wants to send a message to a recipient. An attacker may attempt to:
  - Block the message
  - Intercept the message
  - Modify the message
  - Fabricate an authentic-looking alternate message
- Encryption can address all of these problems

Encryption Terminology

- Sender
- Recipient
- Transmission medium
- Interceptor/intruder
- Encrypt, encode, or encipher
  - Process that hides the meaning of the message
- Decrypt, decode, or decipher
  - Reveal the original message

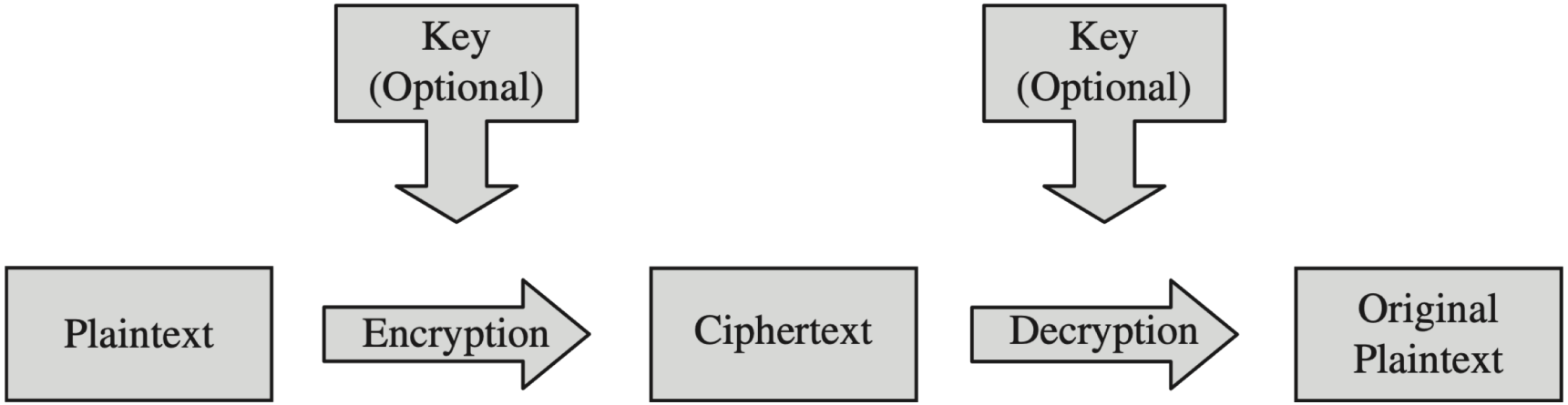
Encryption Terminology

- Cryptosystem
  - A system for encryption and decryption
- Plaintext
  - Original message
- Ciphertext
  - Encrypted message

Encryption Keys

- A cryptosystem involves a set of rules for how to encrypt a plaintext and decrypt the ciphertext
  - Rules == algorithms
- Typically uses a device called a **key (*K*)**
- The resulting ciphertext depends on:
  - The original message
  - The algorithm
  - The key value
    - => the original message is secret, the algorithm typically known
- An encryption key that does not require key is called *keyless cipher*

Encryption/Decryption Process



Basics

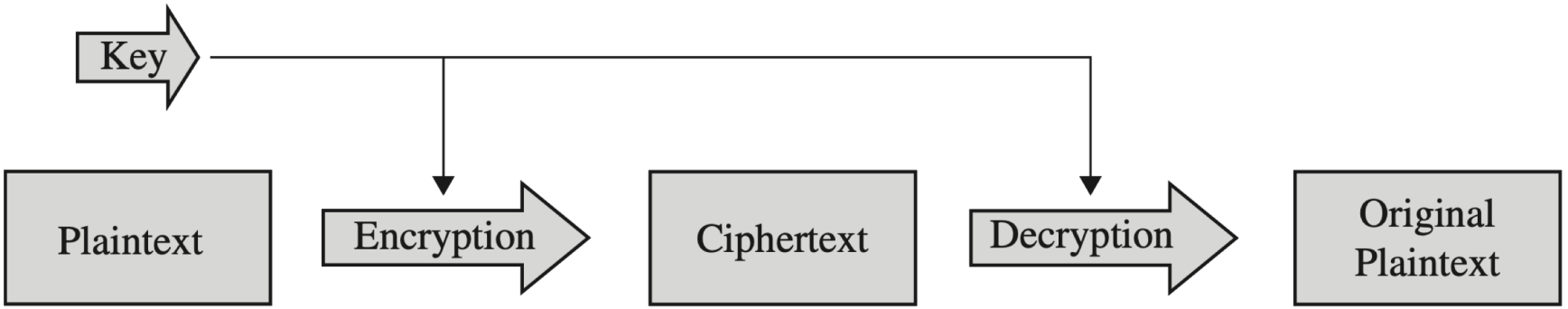
- Notation
  - Secret key K
  - Encryption function EK(P)
  - Decryption function DK(C)
  - Plaintext length typically same as ciphertext length
  - Encryption and decryption are permutation functions (bijections) on the set of all n-bit arrays

http://www.atksolutions.com/articles/basics_on_how_encryption_algorithm_works.html

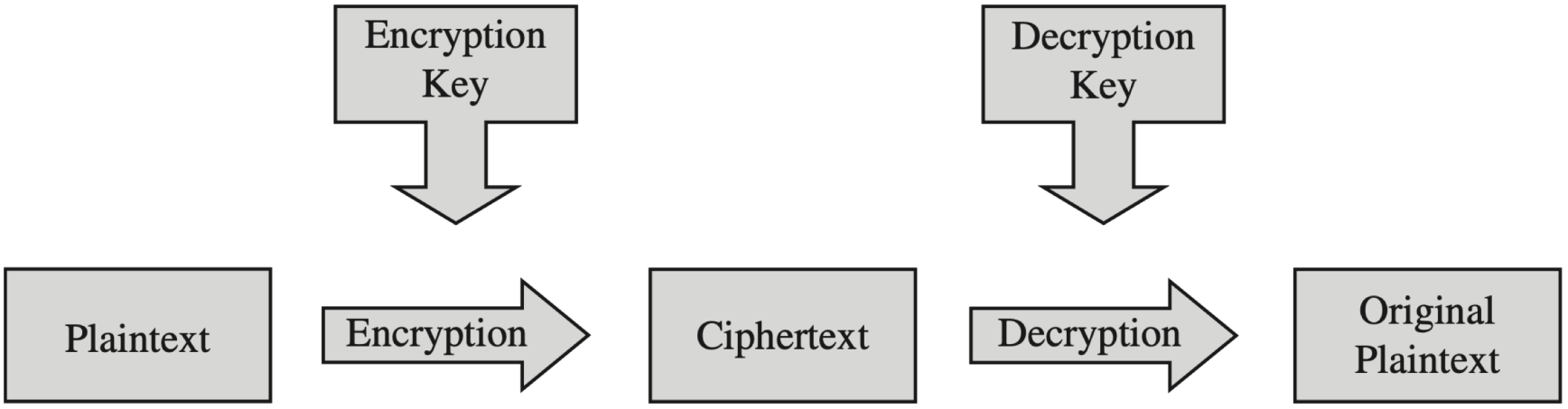
Symmetric and Asymmetric Encryption

- Symmetric encryption uses the same key, K, both to encrypt a message and later to decrypt it
  - Also called single-key or secret key encryption
  - D and E are mirror-image processes
- Asymmetric encryption uses a pair of keys
  - A decryption key, KD, inverts the encryption of key KE, so that $P = D(K_D, E(K_E,P))$

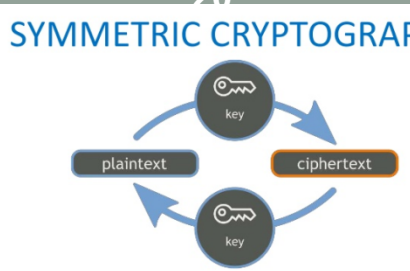
Symmetric vs. Asymmetric



(a) Symmetric Cryptosystem



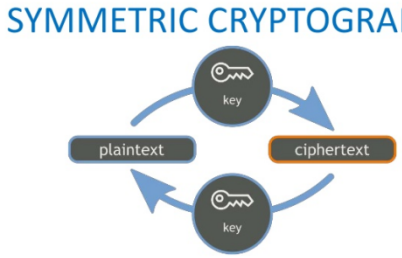
(b) Asymmetric Cryptosystem



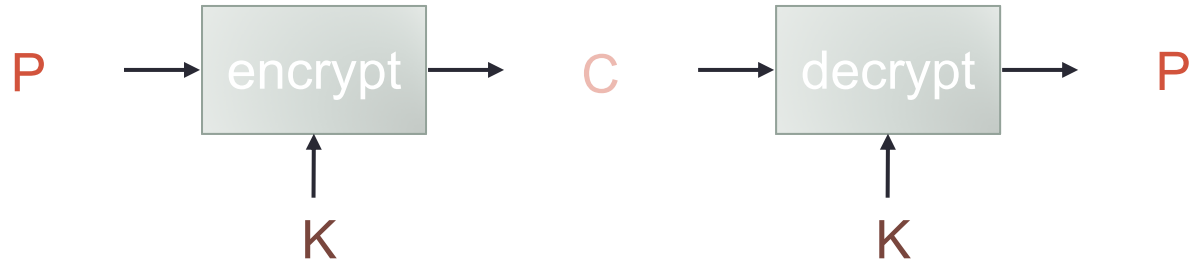
Symmetric Cryptosystem

- Scenario
  - Alice wants to send a message (plaintext P) to Bob.
  - The communication channel is insecure and can be eavesdropped
  - If Alice and Bob have previously agreed on a symmetric encryption scheme and a secret key K, the message can be sent encrypted (ciphertext C)

Symmetric Cryptosystem



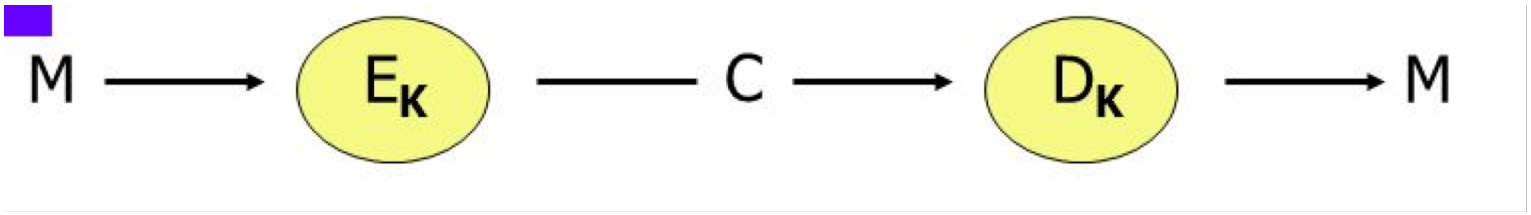
- Issues
  - What is a good symmetric encryption scheme?
  - What is the complexity of encrypting/decrypting?
  - What is the size of the ciphertext, relative to the plaintext?



https://www.slideshare.net/TusharSwami1/cryptography-7296903

Basics

- Efficiency
  - functions EK and DK should have efficient algorithms
- Consistency
  - Decrypting the ciphertext yields the plaintext
  - DK(EK(P)) = P



http://slideplayer.com/slide/10975387/

Cryptanalysis

- A cryptanalyst's chore is to break an encryption
  - Attempts to deduce the original meaning of a ciphertext message
  - Attempts to determine which decrypting algorithm, and key matches the encrypting algorithm t
    - to be able to break other messages encoded in the same way

Cryptanalysis

- An encryption algorithm is called ***breakable*** if it is possible to decrypt the original message
  - given enough time and data,
- However, an algorithm that is theoretically breakable may be impractical to break
  - May take too long
    - Multiple of our lifetimes
- The difficulty of breaking an encryption is called its ***work factor***

Key Exchange

- ***Symmetric*** algorithms use one key, which works for both encryption and decryption
  - Usually, the decryption algorithm is closely related to the encryption one
    - running the encryption in reverse
- Both parties share a secret key
  - they can both encrypt sent information as well as decrypt information from the other

Key Exchange

- As long as the key remains secret, the system also provides authenticity
  - Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly
    - with the shared key

Key Exchange

- How do two users A and B obtain their shared secret key?
  - And only A and B can use that key for their encrypted communications
  - If A wants to share encrypted communication with another user C, A and C need a different shared secret key.
- Managing keys is the major difficulty in using symmetric encryption

Key Exchange

- If we have *n* users, how many keys do we need?
  - *n* users who want to communicate in pairs need n * (n – 1)/2 keys
    - $O(N^2)$
- The number of keys needed increases at a rate proportional to the square of the number of users
- Symmetric encryption systems require a means of key distribution
- How do we solve this?

Key Exchange

- ***Asymmetric or public key*** systems typically have precisely matched pairs of keys.
- The keys are produced together
  - One may be derived mathematically from the other
  - Process computes both keys as a set
- Asymmetric systems good for key management
  - public key may be emailed or post it in a public directory
- Only the corresponding private key can decrypt what has been encrypted with the public key

SYMMETRIC CRYPTOGRAPHY

Data Encryption Standard (DES)

- Symmetric encryption algorithm
- Developed by IBM and adopted by NIST in 1977
- Encrypts 64-bit blocks using 56-bit keys
- Small key space makes exhaustive search attack feasible since late 90s
  - Not secure – should not be used!

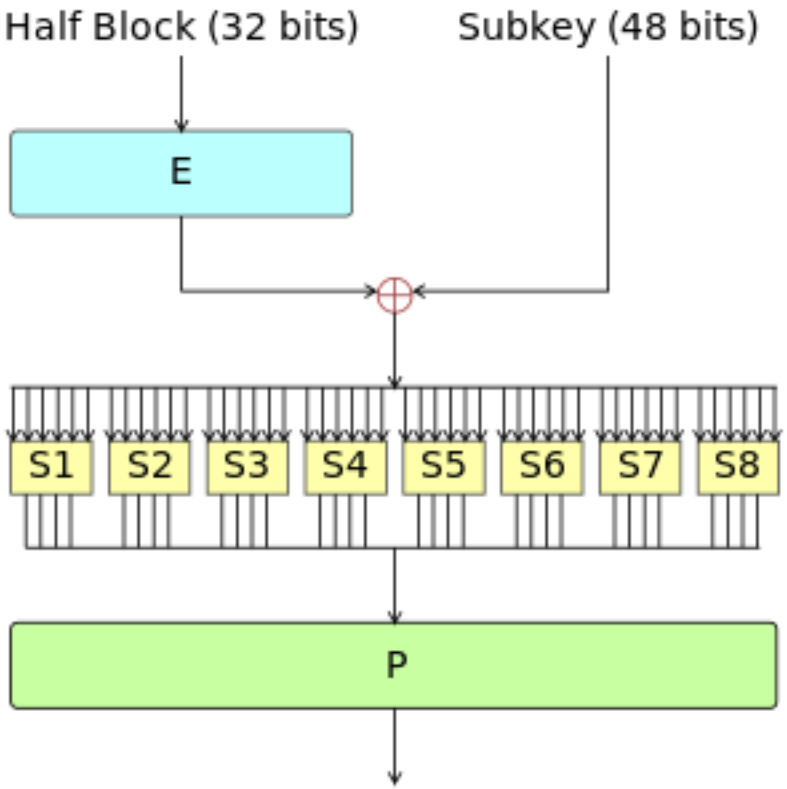
Data Encryption Standard (DES)

- DES is a combination of two fundamental building blocks of encryption:
  - substitution and transposition
- These techniques are repeated one on top of the other, for a total of 16 cycles

Data Encryption Standard (DES)

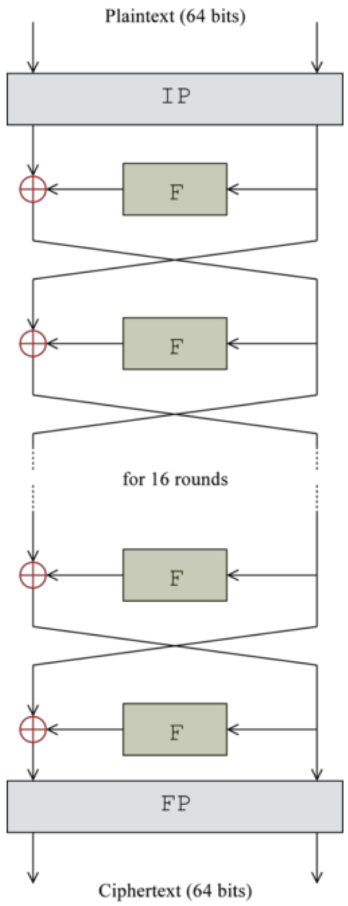
- Each round includes:
  - Substitution:
    - replacing blocks of bits
  - Permutation:
    - Shuffling the bits
  - Transformation:
    - Mingling bits from the key

DES Single Round (Feistel Function)



https://en.wikipedia.org/wiki/Data_Encryption_Standard

DES Algorithm



https://en.wikipedia.org/wiki/Data_Encryption_Standard

DES Algorithm

- DES 56-bit key length is not long enough
  - Not secure
    - Computing power increased rapidly in last few decades
  - How can we make it secure?
    - Explore longer-key version of DES
    - **Problem**: the DES algorithm design is **fixed to a 56-bit key**

Double DES

- Perform two encryptions using two distinct keys:
  - $E(k_2 , E(k_1 ,m))$
- Shown not to be secure [Merkle & Hellman 81]

Triple DES (3DES)

- Nested application of DES with three different keys K_A, K_B, and K_C
- Effective key length is 168 bits
  - making exhaustive search attacks unfeasible
- Ciphertext $C = EK_C(DK_B(EK_A(P)))$;
- Plaintext $P = DK_A(EK_B(DK_C(C)))$
- Equivalent to DES when $K_A=K_B=K_C$ (backward compatible)

Encryption Standards

Form	Operation	Properties	Strength
DES	Encrypt with one key	56-bit key	Inadequate for high-security applications by today's computing capabilities
Double DES	Encrypt with first key; then encrypt result with second key	Two 56-bit keys	Only doubles strength of 56-bit key version
Two-key triple DES	Encrypt with first key, then encrypt (or decrypt) result with second key, then encrypt result with first key (E-D-E)	Two 56-bit keys	Gives strength equivalent to about 80-bit key (about 16 million times as strong as 56-bit version)
Three-key triple DES	Encrypt with first key, then encrypt or decrypt result with second key, then encrypt result with third key (E-E-E)	Three 56-bit keys	Gives strength equivalent to about 112-bit key about 72 quintillion ($72*10^{15}$) times as strong as 56-bit version

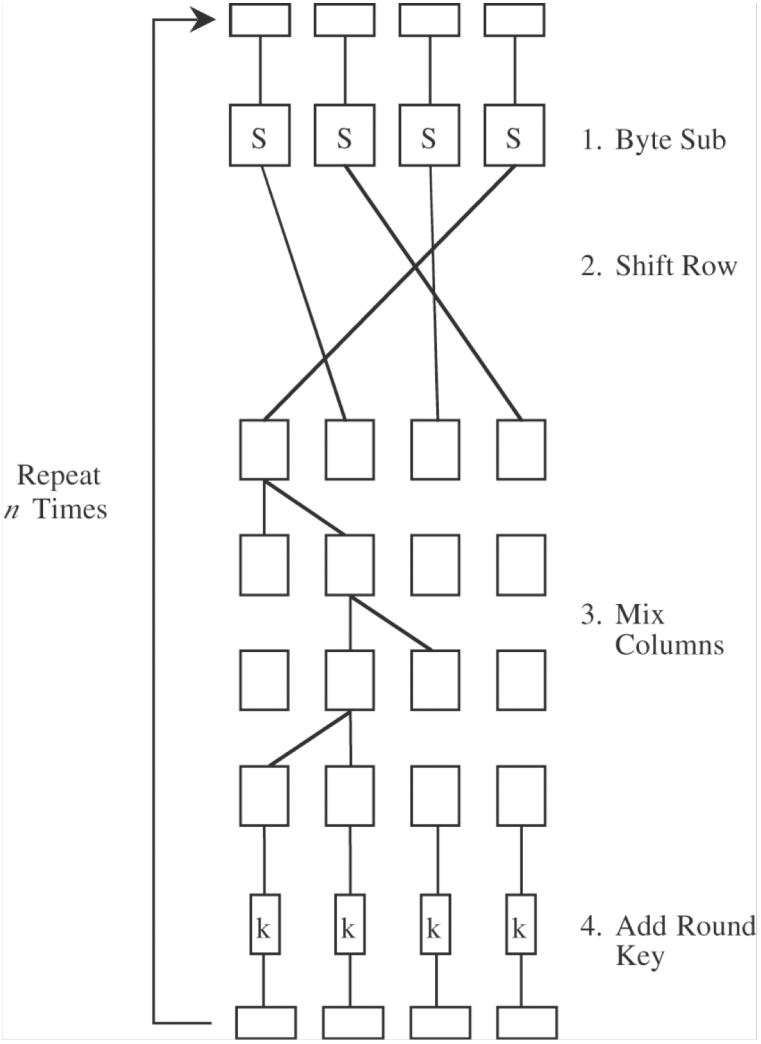
Advanced Encryption Standard (AES)

- Symmetric block cipher
- Developed in 1999 by independent Dutch cryptographers
- Selected by NIST in 2001 through open international competition and public discussion

Advanced Encryption Standard (AES)

- 128-bit blocks and several possible key lengths: 128, 192 and 256 bits
- Exhaustive search attack not currently possible
- AES-256 is the symmetric encryption algorithm of choice
  - Still in common use

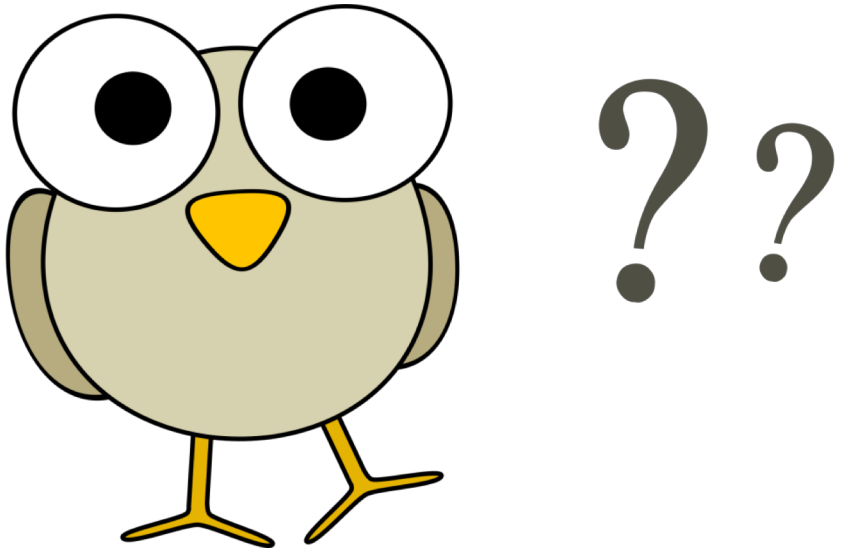
AES: Advanced Encryption System



DES vs. AES

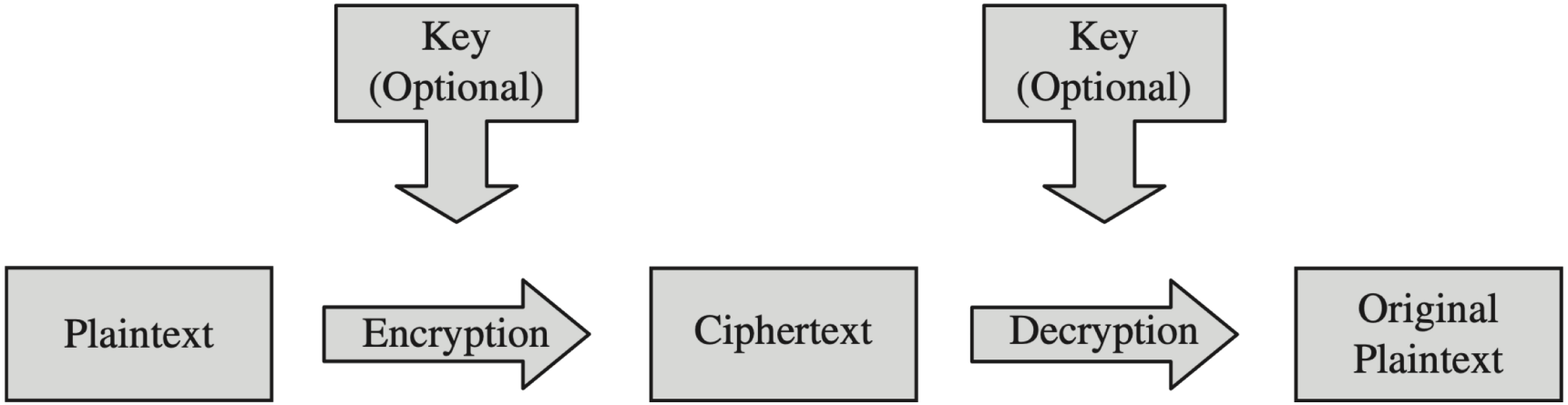
	DES	AES
Date designed	1976	1999
Block size	64 bits	128 bits
Key length	56 bits (effective length); up to 112 bits with multiple keys	128, 192, 256 (and possibly more) bits
Operations	16 rounds	10, 12, 14 (depending on key length); can be increased
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but open public comments and criticisms invited
Source	IBM, enhanced by NSA	Independent Dutch cryptographers

- Questions?

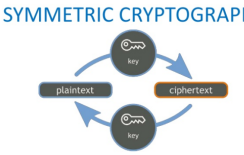


PUBLIC KEY (ASYMMETRIC) ENCRYPTION

Encryption/Decryption Process



Reminder - Symmetric Cryptosystem

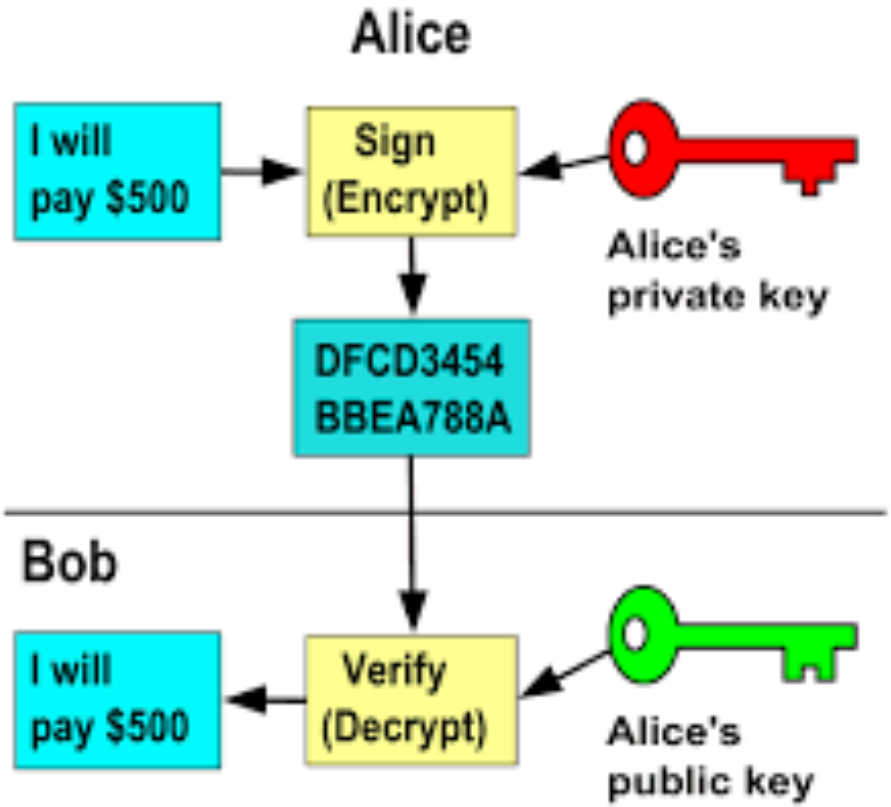


- Scenario
  - Alice wants to send a message (plaintext P) to Bob.
  - The communication channel is insecure and can be eavesdropped
  - If Alice and Bob have previously agreed on a symmetric encryption scheme and a secret key K, the message can be sent encrypted (ciphertext C)

Public Key (Asymmetric) Cryptography

- Instead of two users sharing one secret key, each user has two keys: one public and one private
- Messages encrypted using the user's public key can only be decrypted using the user's private key, and vice versa
  - P = D(Kpriv,E(Kpub,P)) or
  - P = D(Kpub,E(Kpriv,P))

Public Key Encryption



https://commons.wikimedia.org/wiki/File:Public_key_signing.svg

Public Key Encryption

- A cryptographic system that uses pairs of keys
  - public keys which may be disseminated widely
    - Any person can encrypt the message
  - private keys which are known only to the owner
    - Message can only be decrypted with this key
- Analogous to a self-closing door
  - Need key to open it
  - Closing it shuts it automatically

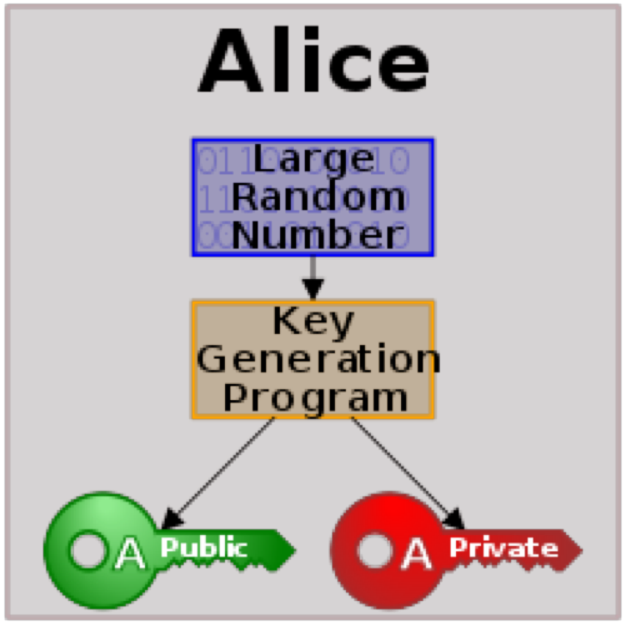
Public Key Encryption

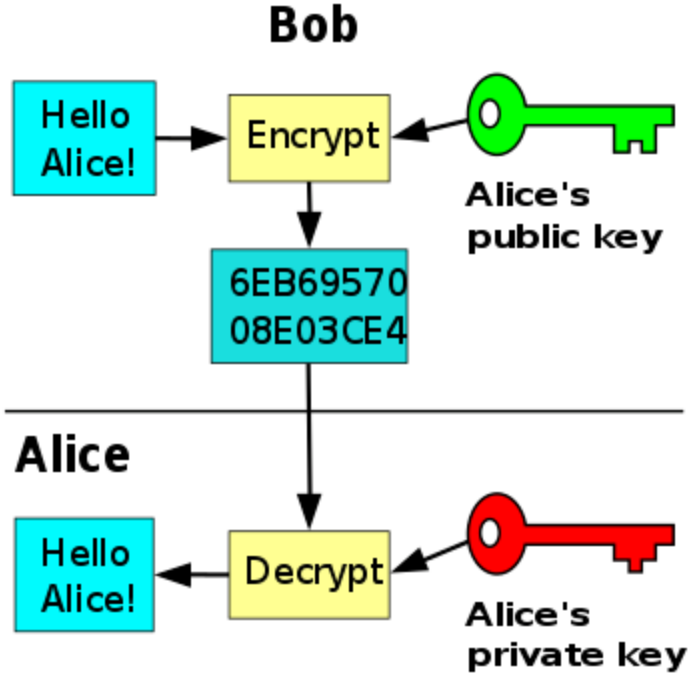
- Accomplishes two functions: authentication and encryption
- Authentication: the public key verifies that a holder of the paired private key sent message
  - Decryption will fail otherwise
- Encryption: only the paired private key holder can decrypt the encrypted message

Public Key Encryption

- Why does it work?
- It is not feasible to compute the private key
  - From knowledge of its paired public key
- Therefore, only the private key is kept private
  - The public key can be openly distributed without compromising security
- Public key cryptography relies on math problems that have no efficient solution

Public Key Encryption





https://en.wikipedia.org/wiki/Public-key_cryptography

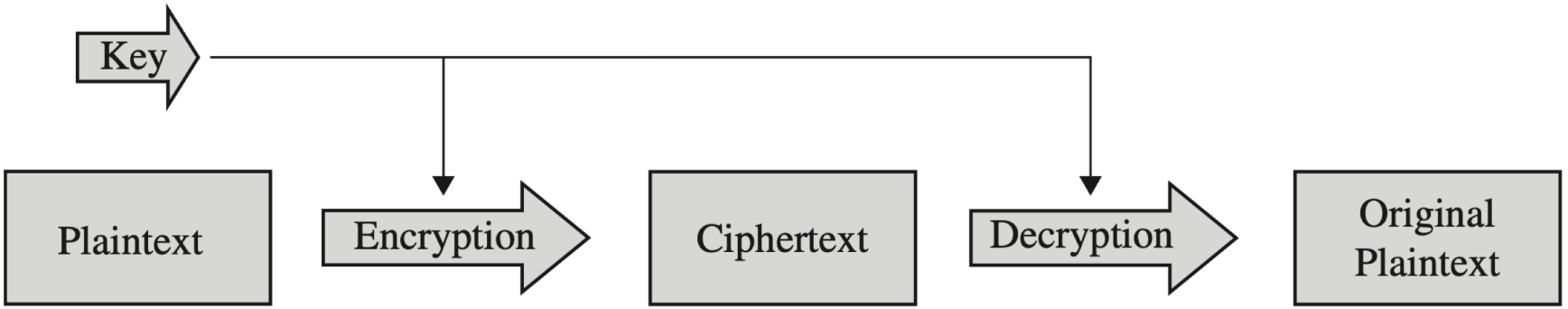
Public Key Encryption

- Often used to secure communication
  - Over the internet, open networks
  - Typically used for key exchange

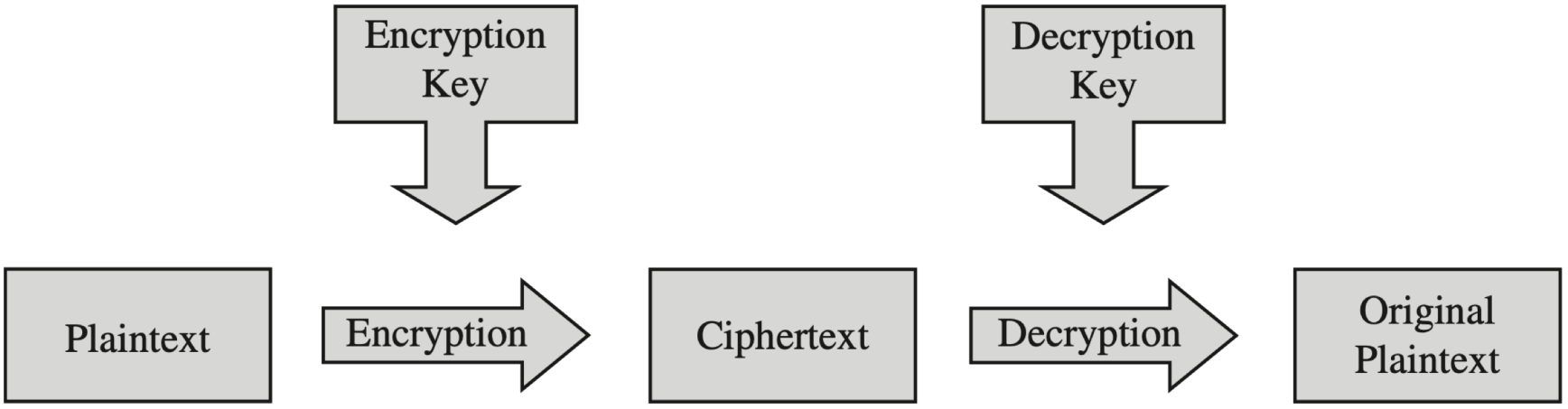
Secret Key vs. Public Key Encryption

	Secret Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Key size (bits)	56–112 (DES), 128–256 (AES)	Unlimited; typically no less than 256; 1000 to 2000 currently considered desirable for most uses
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse. Secrecy and integrity of data, from single characters to blocks of data, messages and files	Key exchange, authentication, signing
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow, typically by a factor of up to 10,000 times slower than symmetric algorithms

Symmetric vs. Asymmetric



(a) Symmetric Cryptosystem



(b) Asymmetric Cryptosystem

Symmetric vs. Asymmetric

- The critical difference between symmetric and asymmetric is that symmetric uses a single key for both encryption and decryption
  - whereas asymmetric uses complementary keys

Rivest-Shamir-Adelman Public Key Encryption (RSA)

- A public key system
- Based on an underlying hard problem
  - Makes is hard to break the system
    - Get the private key
- RSA uses two keys, *d* and e, for decryption and encryption

Rivest-Shamir-Adelman Public Key Encryption (RSA)

- The two keys can be used interchangeably:
- C = RSA(P,*e*) - *e* can be either Kpriv or Kpub

- Then
- P = RSA(RSA(P,*e*),*d*) where *d* is the other key

Rivest-Shamir-Adelman Public Key Encryption (RSA)

- The keys can be 256 to 1000s of bits
- The relationship between the keys relies on the fact that a large number is the product of two large prime numbers.

RSA Runtime

- Keys are long: 256 is the minimum
- Encryption is done by exponentiation
  - In contrast to substitution and transposition used in symmetric algorithm
    - Significantly slower to run on a computer
- RSA runtime significantly longer than DES or AES

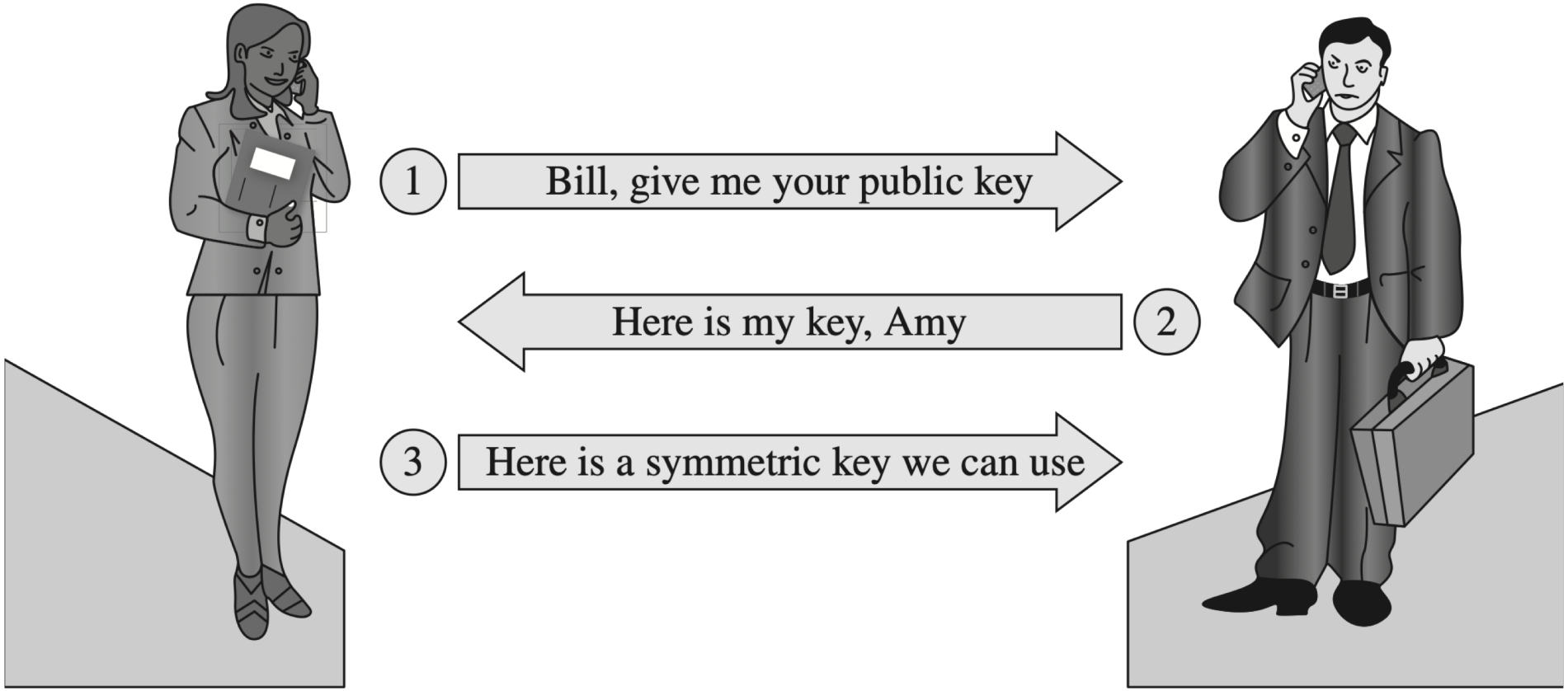
Secret Key vs. Public Key Encryption

- Symmetric and asymmetric algorithms have complementary strengths and weaknesses
- Used for different purposes
  - in concert with each other

Secret Key vs. Public Key Encryption

	Secret Key (Symmetric)	Public Key (Asymmetric)
Number of keys	1	2
Key size (bits)	56–112 (DES), 128–256 (AES)	Unlimited; typically no less than 256; 1000 to 2000 currently considered desirable for most uses
Protection of key	Must be kept secret	One key must be kept secret; the other can be freely exposed
Best uses	Cryptographic workhorse. Secrecy and integrity of data, from single characters to blocks of data, messages and files	Key exchange, authentication, signing
Key distribution	Must be out-of-band	Public key can be used to distribute other keys
Speed	Fast	Slow, typically by a factor of up to 10,000 times slower than symmetric algorithms

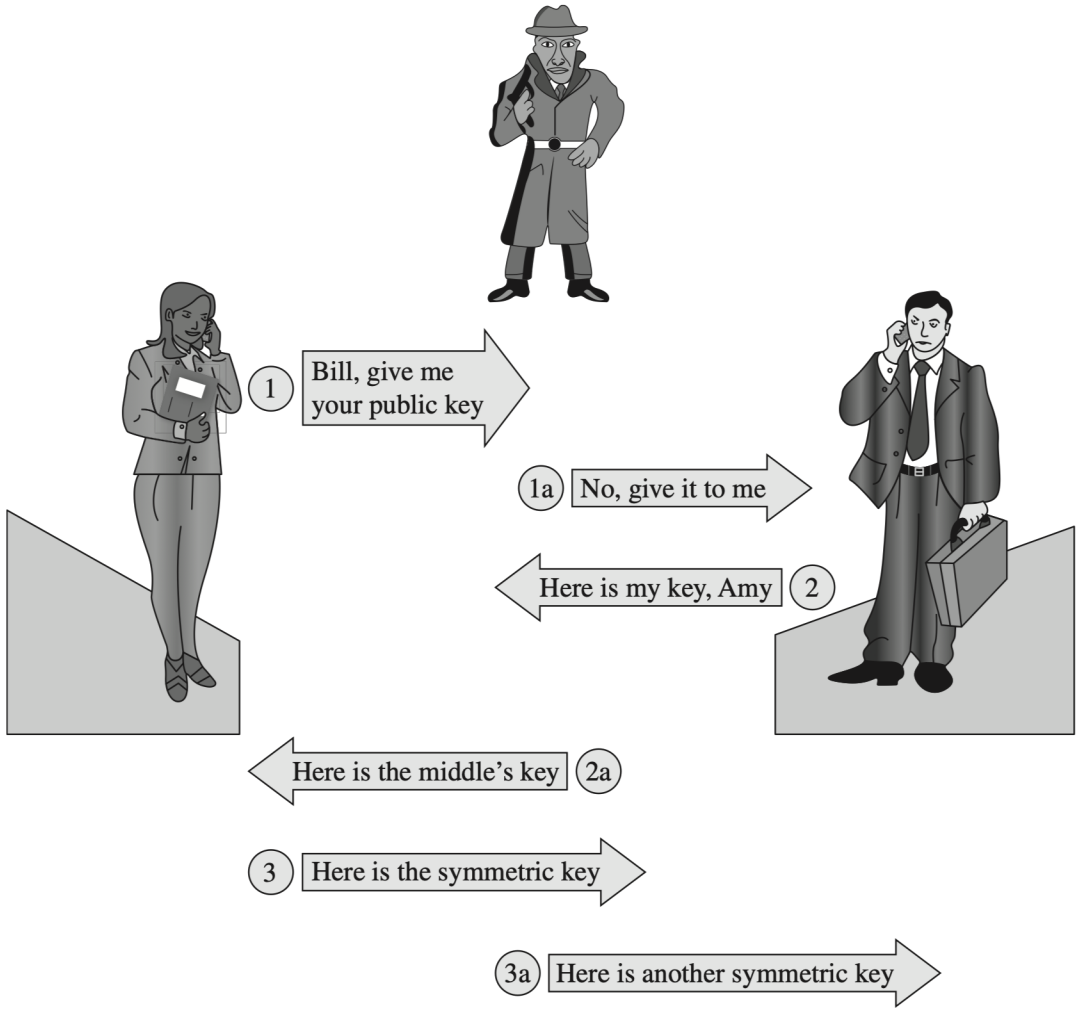
Public Key to Exchange Secret Keys



Key Exchange Man in the Middle

- What if we have a man in the middle attack?
  - Revised protocol is needed

Key Exchange Man in the Middle



Revised Key Exchange Protocol

- Similar to original mechanism, but key is sent in two batches
  - Half every time
- Intruder, can certainly intercept both public keys and substitute his own
- However, the attacker cannot take half the result, decrypt it using his private key, and re-encrypt it under Bill's key
  - Bits cannot be decrypted one by one and reassembled

Revised Key Exchange Protocol

- A provides their public key – anyone can access it
- B provides their public key – anyone can access it
- A encrypts a symmetric key using B's public key and sends half the bits to B
- B confirms that he has received half the bits.
  - B encrypts a random number with A's public key and sends half the bits to A.
- A sends the other half of the encrypted bits.

Revised Key Exchange Protocol

- B combines the two sets of bits and decrypts them using B's private key.
  - B sends the other half of the encrypted random number.
- A combines the two parts of the random number and decrypts it with A's private key.
  - A then uses the symmetric key to encrypt the random number and sends it to B.
- B decrypts the random number with the symmetric key.
  - A match to the original random number confirms the secure exchange.

Alternative Key Exchange Protocol

1. A sends to B

$E(K_{pub\text{-}B},(E(K_{priv\text{-}A},K))$ where K is the symmetric key

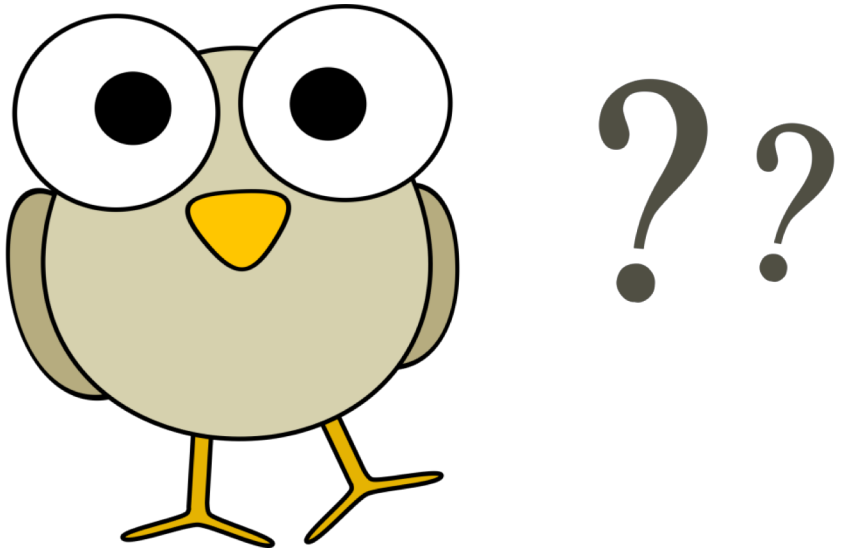
2. B uses $K_{priv\text{-}B}$ to decrypt the $K_{pub\text{-}B}$ encryption
3. B uses $K_{pub\text{-}A}$ to decrypt the $K_{priv\text{-}A}$ encryption and obtain K

Once the symmetric key has been successfully exchanged, it can be used for the rest of the communication.

Revised Key Exchange Protocol

- Secure key exchange is complicated
- Many alternative secure protocols exist
  - Protocols need to be proven secure
  - New attacks introduced continuously

- Questions?



WHY JOHNNY CAN'T ENCRYPT

Whitten and Tygar, 1999

Research Question

- If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, will PGP's current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides to give up on using PGP after all?

Research Question

- Average people never acquired PGP with that intent, nor discovered the encryption and authentication features baked into Outlook, because they were never introduced to the underlying concepts

- https://www.wired.com/insights/2012/10/why-johnny-cant-syndicate/

Conclusion

- It may take a long time, and require a lot of education, to add the concepts that underly privacy and authentication

- https://www.wired.com/insights/2012/10/why-johnny-cant-syndicate/

Questions?