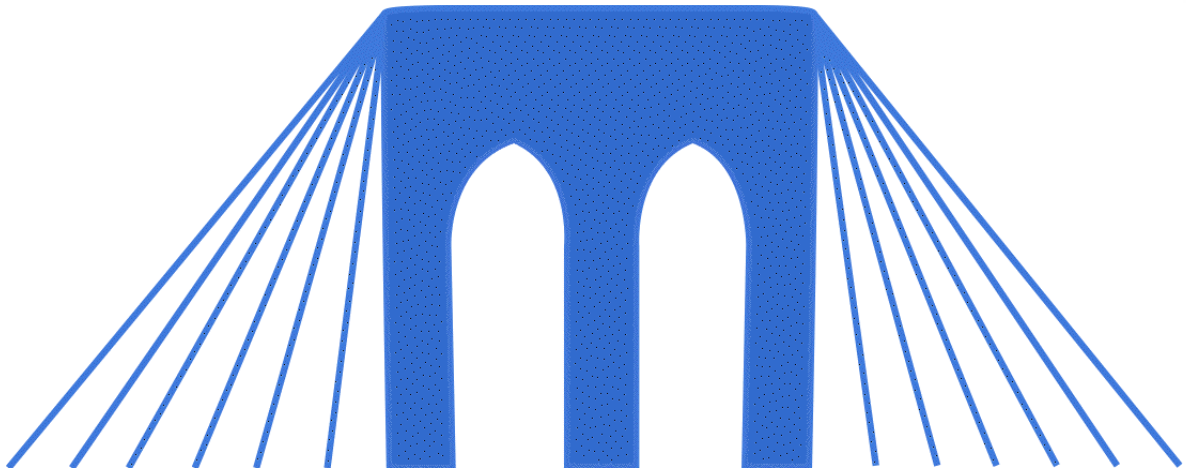
Bridges To Computing



General Information:

- This document was created for use in the "Bridges to Computing" project of Brooklyn College.
- You are invited and encouraged to use this presentation to promote computer science education in the U.S. and around the world.
- For more information about the Bridges Program, please visit our website at: http://bridges.brooklyn.cuny.edu/

Disclaimers:

- **IMAGES**: All images in this presentation were created by our Bridges to Computing staff or were found online through open access media sites and are used under the Creative Commons Attribution-Share Alike 3.0 License. If you believe an image in this presentation is in fact copyrighted material, never intended for creative commons use, please contact us at http://bridges.brooklyn.cuny.edu/ so that we can remove it from this presentation.
- **LINKS**: This document may include links to sites and documents outside of the "Bridges to Computing" domain. The Bridges Program cannot be held responsible for the content of 3rd party sources and sites.

Introduction to Cryptology II

Cryptography
&
Cryptanalysis

M. Meyer
Bridges To Computing
2010

Modern Cryptography - Purpose

- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptographic Algorithms

- There are several ways of classifying cryptographic algorithms. We will categorized them by the number of keys that are employed for encryption and decryption
  - Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.
  - Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.
  - Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

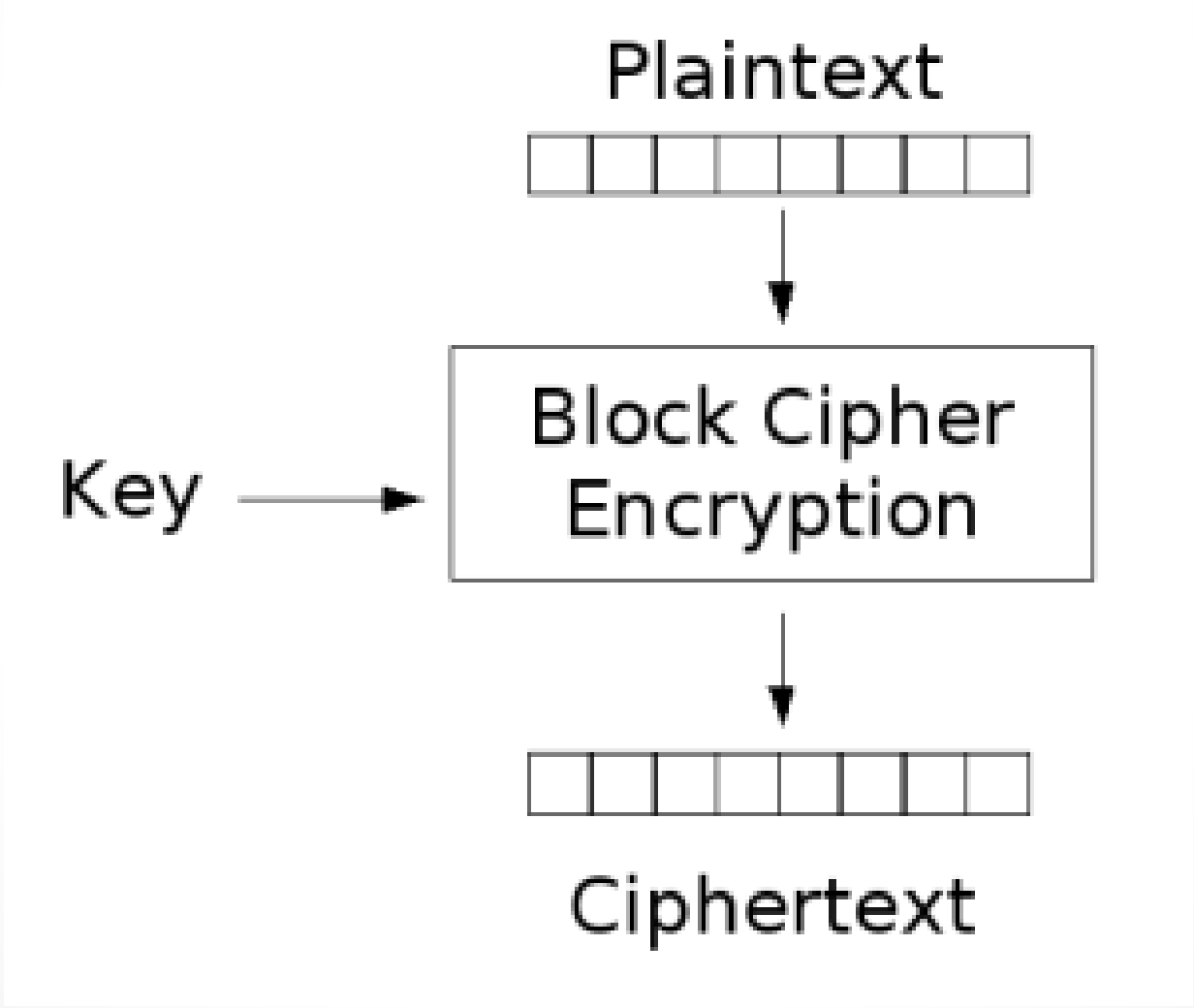
B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

SKC - Secret Key

- With secret key cryptography, a single key is used for both encryption and decryption. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.
-
- SKC algorithms fall into two general groups: Block Ciphers and Stream Ciphers.

SKC - Block Ciphers



Modern PKC Standards

- Data Encryption Standard (DES) and it's replacement Triple-DES (3DES) are the two most well known PKC standards.
- They are used for creating passwords for computers and for low-level security protocols for network communication.
- They are breakable and vulnerable to specific kinds of attacks.
  - If I can get enough of the messages that are encoded with the key.
  - If the text I am looking to find is an English word of phrase.

The problem of the key

- Even if I am going to use a one-time pass encryption key (in theory, unbreakable) to send you a message, I have a problem.... namely, you will need the key yourself, to decode the message.
- How then, can I get you the key safely?
- This problem was unanswerable until the late 1970's and the world had the problem that if a spy managed to steal the codebook from you, then all of your messages could then be read.

PKC - Public Key

- "Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years.
- Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976.
- Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.
- PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to computer whereas their inverse function is relatively difficult to compute. Let me give you two simple examples:"

PKC continued

Multiplication vs. factorization:

- Suppose I tell you that I have two numbers, 9 and 16, and that I want to calculate the product; it should take almost no time to calculate the product, 144.
- Suppose instead that I tell you that I have a number, 144, and I need you tell me which pair of integers I multiplied together to obtain that number.
- You will eventually come up with the solution but whereas calculating the product took milliseconds, factoring will take longer because you first need to find the 8 pair of integer factors and then determine which one is the correct pair.

PKC continued

Exponentiation vs. logarithms:

- Suppose I tell you that I want to take the number 3 to the 6th power; again, it is easy to calculate 3^6=729.
- But if I tell you that I have the number 729 and want you to tell me the two integers that I used, x and y so that log(x) 729 = y, it will take you longer to find all possible solutions and select the pair that I used.
- There may in fact be more then one pair.

PKC - Standards

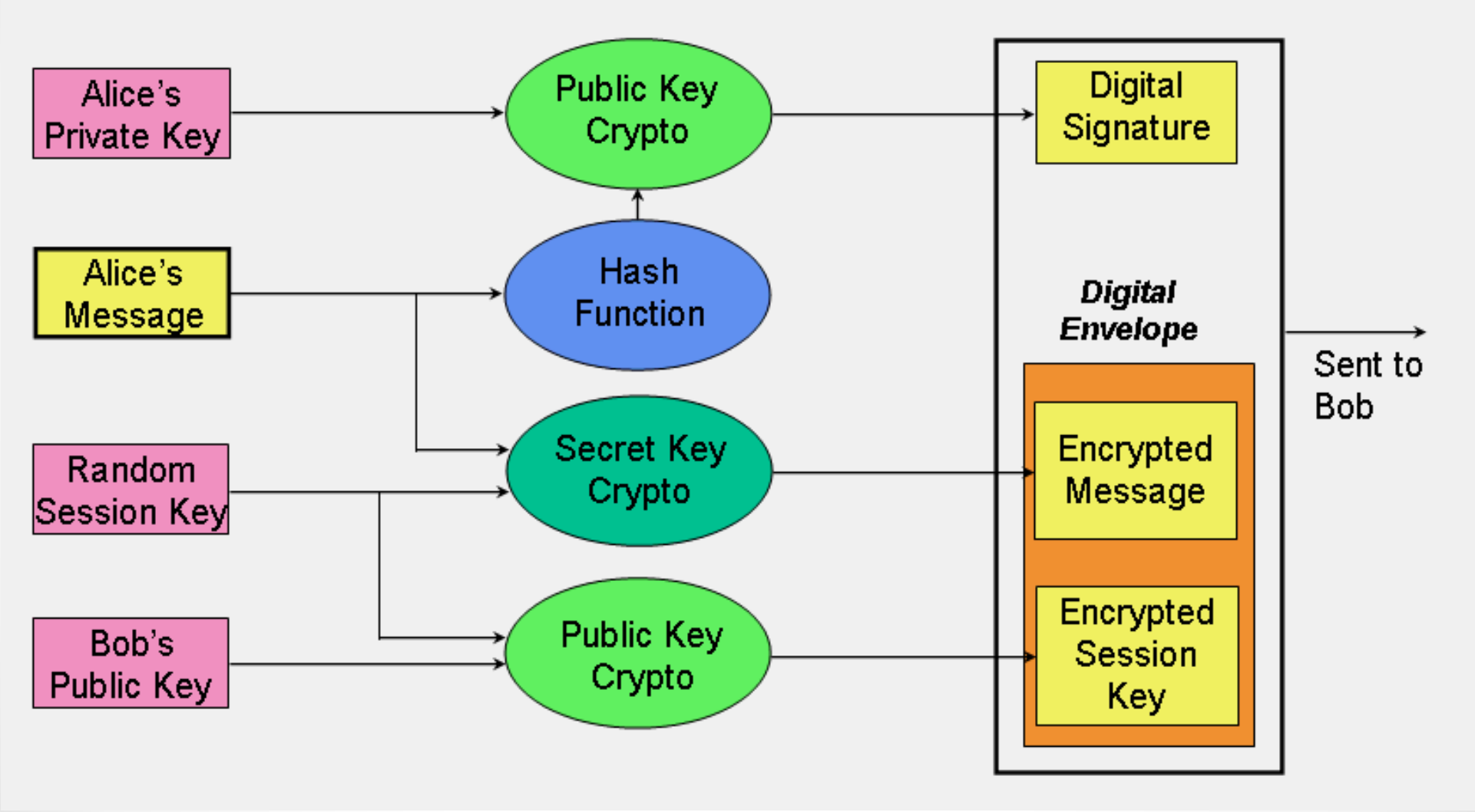
- The first, and still most common, PKC implementation, is named for the three MIT mathematicians who developed it — Ronald **R**ivest, Adi **S**hamir, and Leonard **A**dleman.
- RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data.
- The main idea, is that each of the keys is derived from the factoring of an extremely large prime number.
- AND what is encoded with one key, can only be decoded with the other.

Hash Algorithms

- Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

- Popular Hash Algorithm MD5.

Why 3 types?


Alice's Private Key
Public Key Crypto
Digital Signature
Alice's Message
Hash Function
Digital Envelope
Sent to Bob
Random Session Key
Secret Key Crypto
Encrypted Message
Bob's Public Key
Public Key Crypto
Encrypted Session Key

Trust Models (1)

- Secure use of cryptography requires trust.
- SKC can ensure message confidentiality and hash codes can ensure integrity, but none of this works without trust.
- In SKC, Alice and Bob had to share a secret key. PKC solved the secret distribution problem, but how does Alice really know that Bob is who he says he is?
- Just because Bob has a public and private key, and purports to be "Bob," doesn't mean that he is Bob.

Trust Models

There are a number of trust models employed by various cryptographic schemes:

- PGP- The web of trust employed by Pretty Good Privacy (PGP) users, who hold their own set of trusted public keys.
- Kerberos- a secret key distribution scheme using a trusted third party.
- Certificates- which allow a set of trusted third parties to authenticate each other and, by implication, each other's users

The End