

*A&N Associates, Inc.*

**A Partnership  
To Secure Your Future**

**Basics of Cryptography**

# Definition of Cryptography

- **Conversion of plain text data into a secret code**

We will announce  
the merger at noon  
on Friday

Plain Text Data



px pbdd tgghnvx  
max fxlzxl tm ghhg  
hg ylbwtr

Secret Code

# Brief History

- **Dates as far back as 1900 B.C in Egypt**
- **Julius Caesar (100-44 B.C.) used simple substitution**
  - For example, substitute each letter in the alphabet with a different letter

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

# Brief History (cont.)

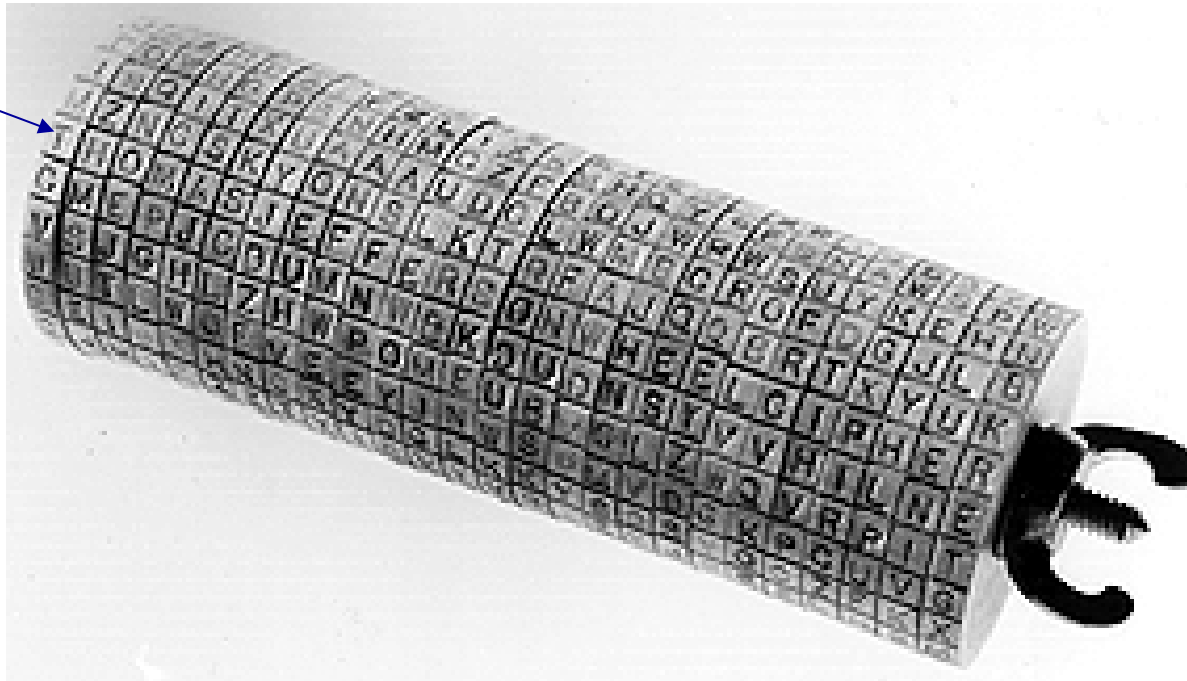
- **Sir Francis Bacon (1623) – Bi-literal cipher**

A B C D E F  
Aaaaa aaaaab. aaaba. aaabb. aabaa. aabab.  
G H I K L M  
aabba aabbb abaaa. abaab. ababa. ababb.  
N O P Q R S  
abbaa. abbab. abbaa. abbbb. baaaa. ba aab.  
T V W X Y Z  
baaba. baabb. babaa. babab. babba. babbb.

# Brief History (cont.)

- **Thomas Jefferson (1790) – Wheel Cipher**

Read this  
line on the  
wheel



# Brief History (cont.)

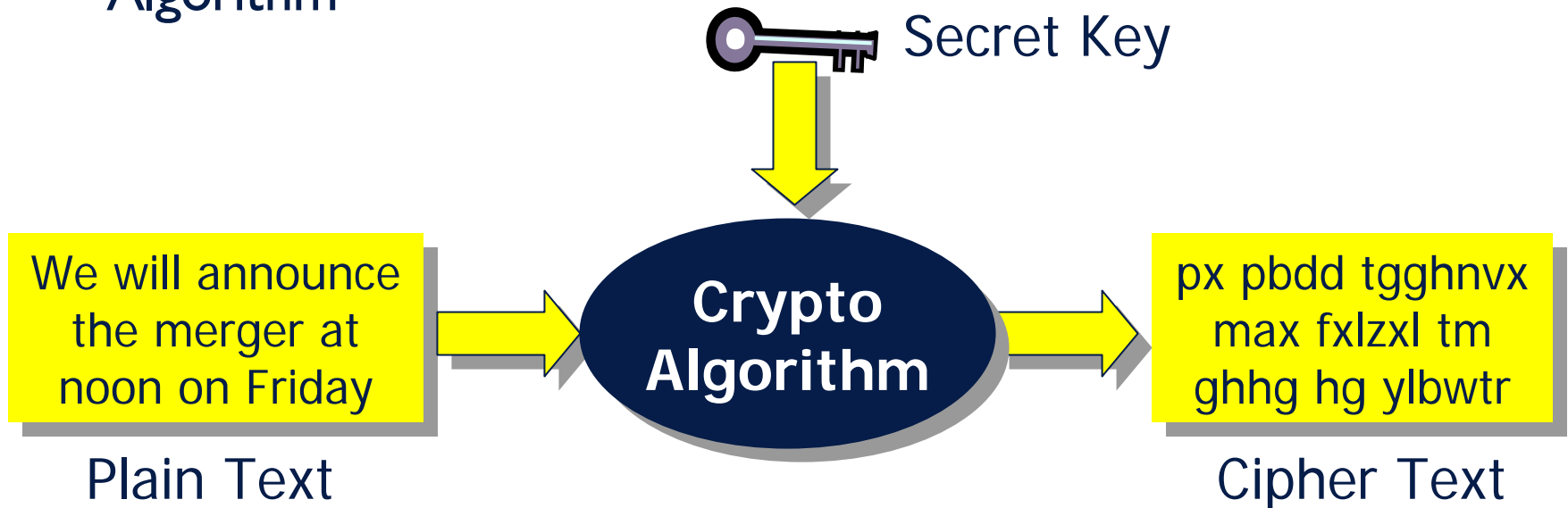
- **William Frederick Friedman – Father of US Cryptanalysis**
  - US Government cryptanalyst
  - 1918 – Index of Coincidence and its Applications in Cryptography
- **WWII Code Machines:**
  - Germany's Enigma
  - Japan's Purple

# Brief History (cont.)

- **1970s**
  - 1976 – DES standardized
  - 1976 – Public key cryptography introduced
  - 1977 – RSA cipher introduced
- **1980s – Stronger ciphers (128 bit) introduced (e.g., IDEA)**
- **1990s – Integration of cryptography into commercial applications**
- **Post 2K:**
  - AES standardized to replace DES
  - Emergence on the use of “elliptic curve” cryptography

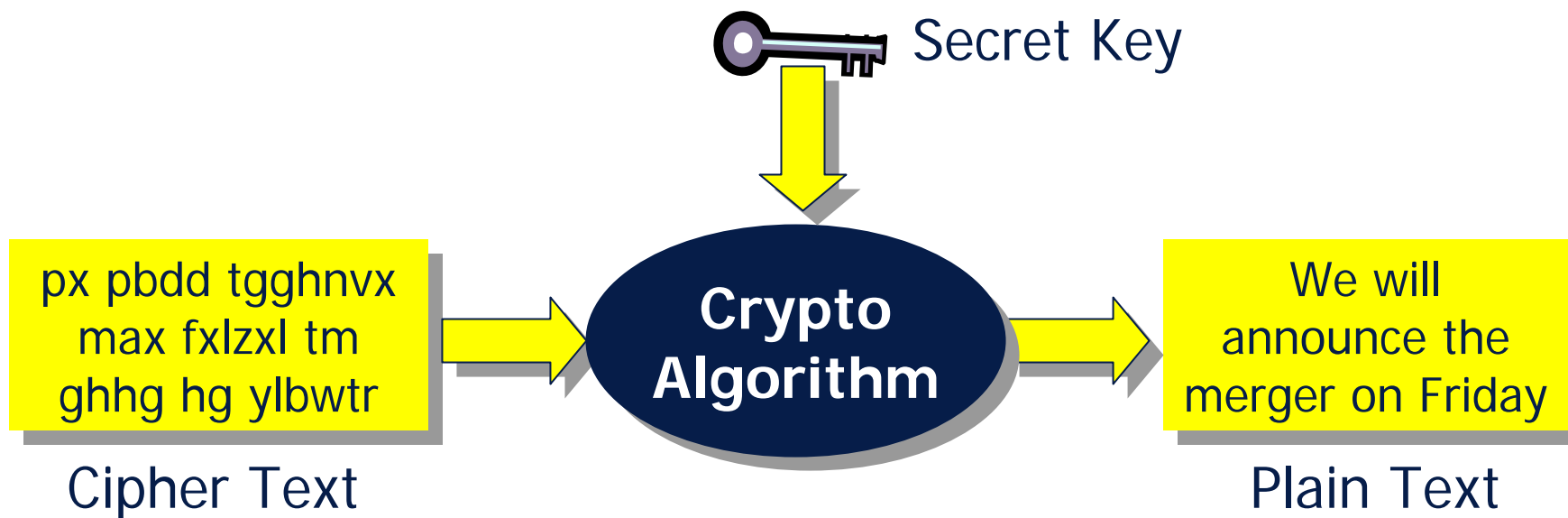
# Encrypting Data

- **Encrypting data primarily requires two components**
  - Secret key
  - Algorithm



# Decrypting Data

- Reverse process of encryption

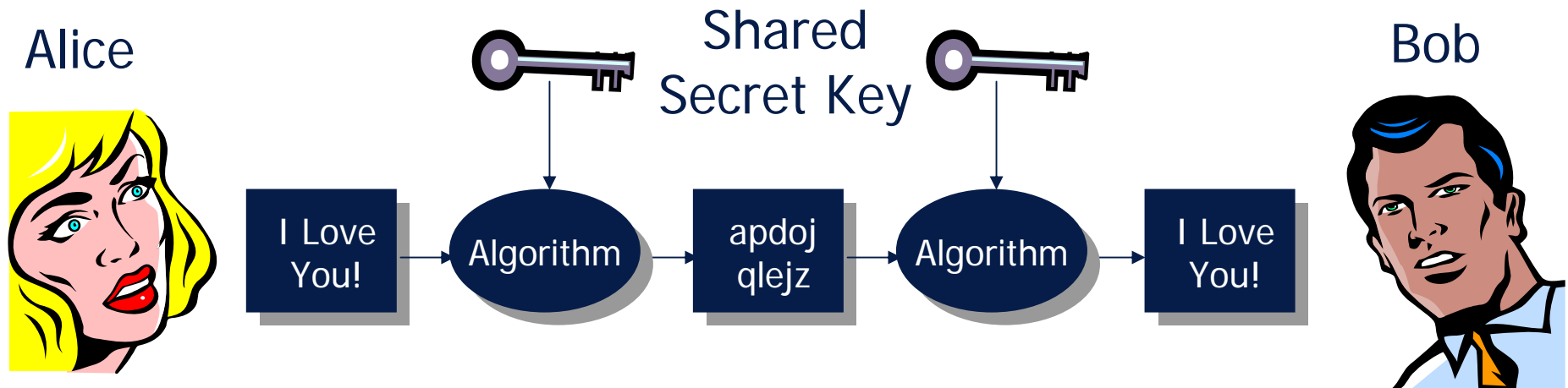


# Types of Cryptographic Algorithms

- **Symmetric**
- **Asymmetric**
- **One-Way Hashes**

# Symmetric Cryptography

- Use the same secret key to encrypt and decrypt data



# Symmetric Cryptography: Pros and Cons

- **Pros:**

- Fast
- Short keys
- Well known
- Key generation simple

- **Cons:**

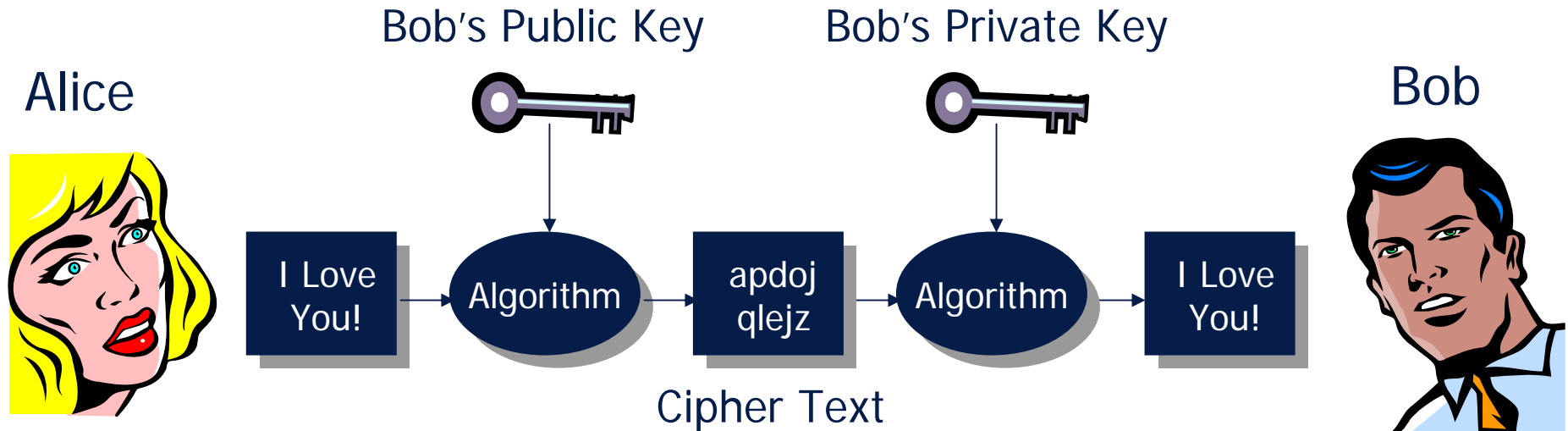
- Secrecy of keys
- Mgmt of keys
- Nos. of keys

# Asymmetric Cryptography

- **Use one key for encryption, and one key for decryption**
  - One key is considered the private (secret) key, while the other is considered the public key
  - Keys are mathematically related to one another

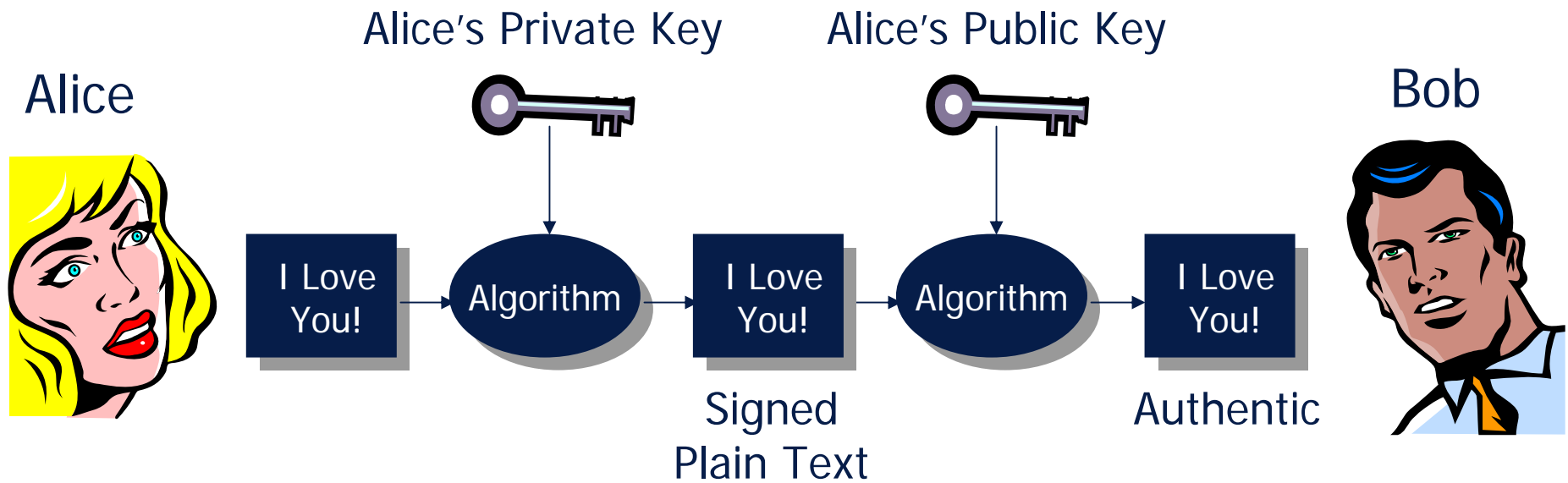
# Asymmetric Cryptography

- An example (encrypting):



# Asymmetric Cryptography

- An example (signing):



# Asymmetric Cryptography: Pros and Cons

- **Pros:**

- No shared secrets
- Key mgmt easier
- Provides secrecy and authenticity

- **Cons:**

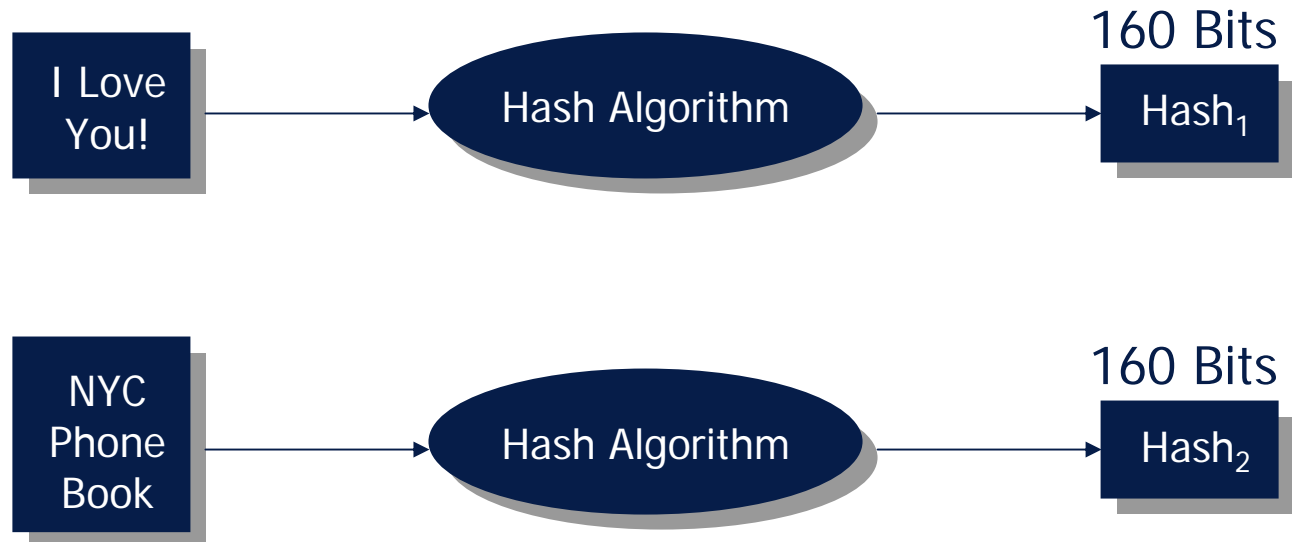
- Slow
- Large keys
- Key generation is more difficult

# One-Way Hashes

- **Calculates a fixed size value using input of any size**
  - Result is typically 128 or 160 bits
  - Newer algorithms will produce larger outputs
- **Key Properties:**
  - No two results are the same
  - One-way function (i.e., cannot determine input from output)

# One-Way Hashes

- **An example:**



$Hash_1 \neq Hash_2$

*Any change to input  
produces new output*

**DATA INTEGRITY**

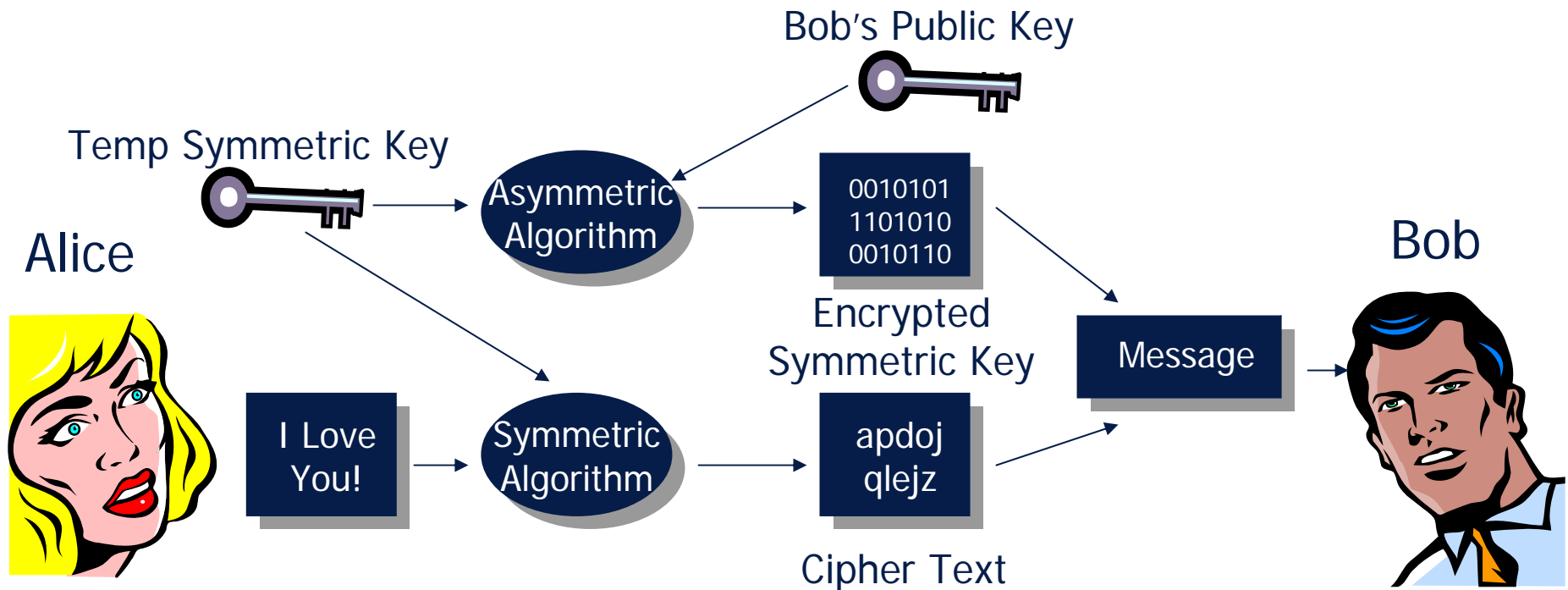
*AN Associates, Inc.*

# Combining Cryptographic Methods

- **Encryption:**
  - Encrypt data with a temporary symmetric key
  - Encrypt symmetric key to recipient using recipient's public key
- **Decryption:**
  - Decrypt temporary symmetric key using own private key
  - Decrypt message using symmetric key

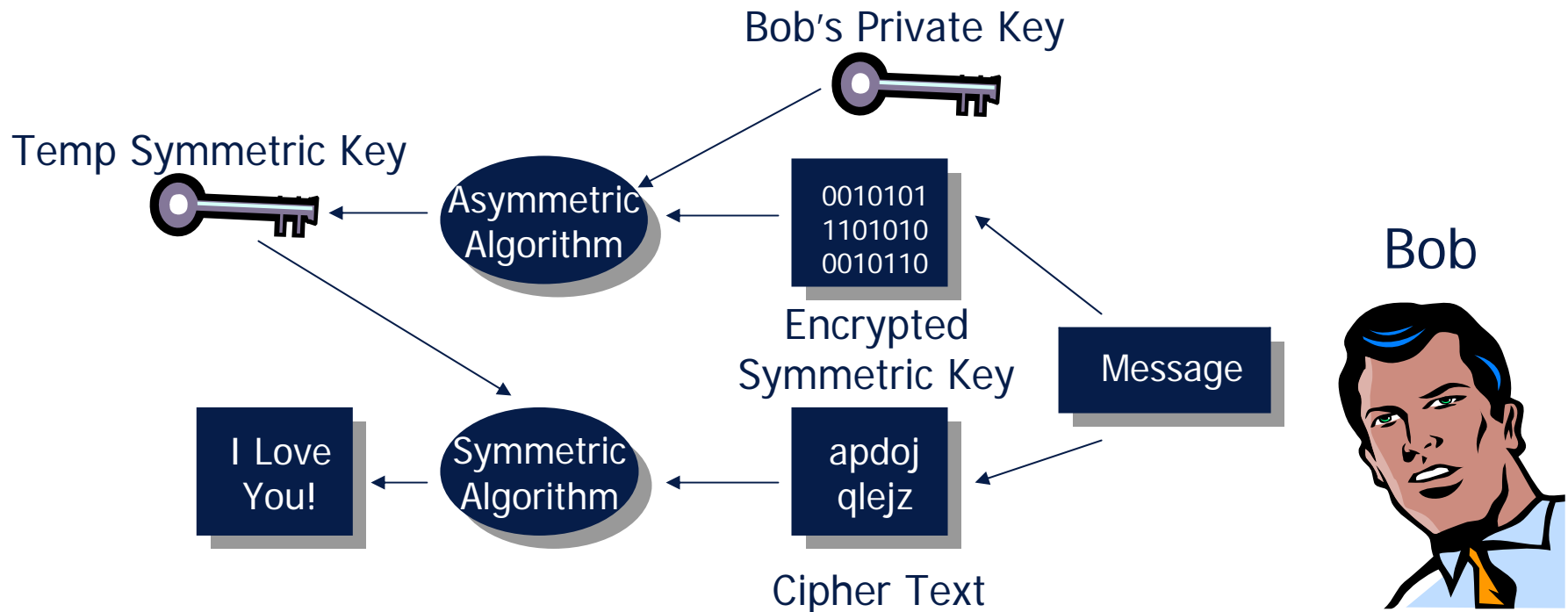
# Combining Cryptographic Methods

- **Encryption (An Example):**



# Combining Cryptographic Methods

- **Decryption (An Example):**



# Combining Cryptographic Methods

- **Signing:**

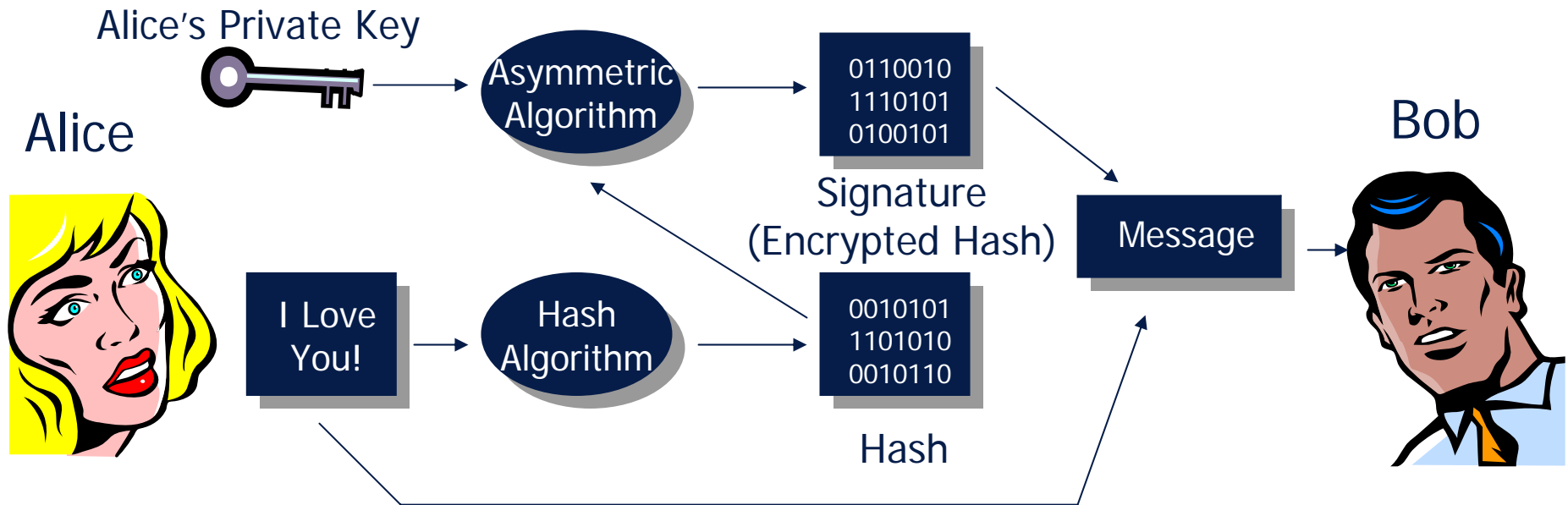
- Hash the data to be signed (data integrity)
- Sign the hash (authentication)

- **Verification:**

- Verify signature on hash (authentication)
- Verify hash against a calculated hash of data (data integrity)

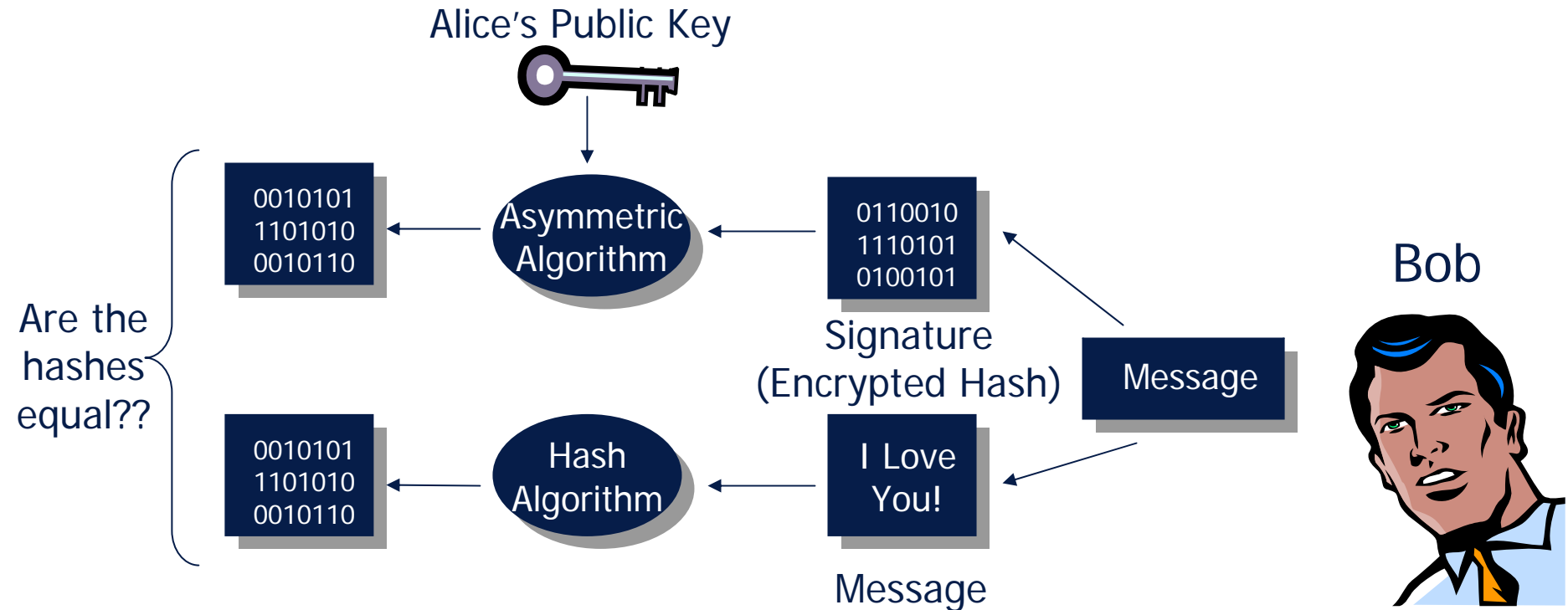
# Combining Cryptographic Methods

- **Signing (An Example):**



# Combining Cryptographic Methods

- **Signature Verification (An Example):**



# Summary

- **Different types of cryptographic algorithms address different requirements**
- **Each type of algorithm has its set of pros and cons**
- **Combining types of algorithms provides complete and useful solutions**