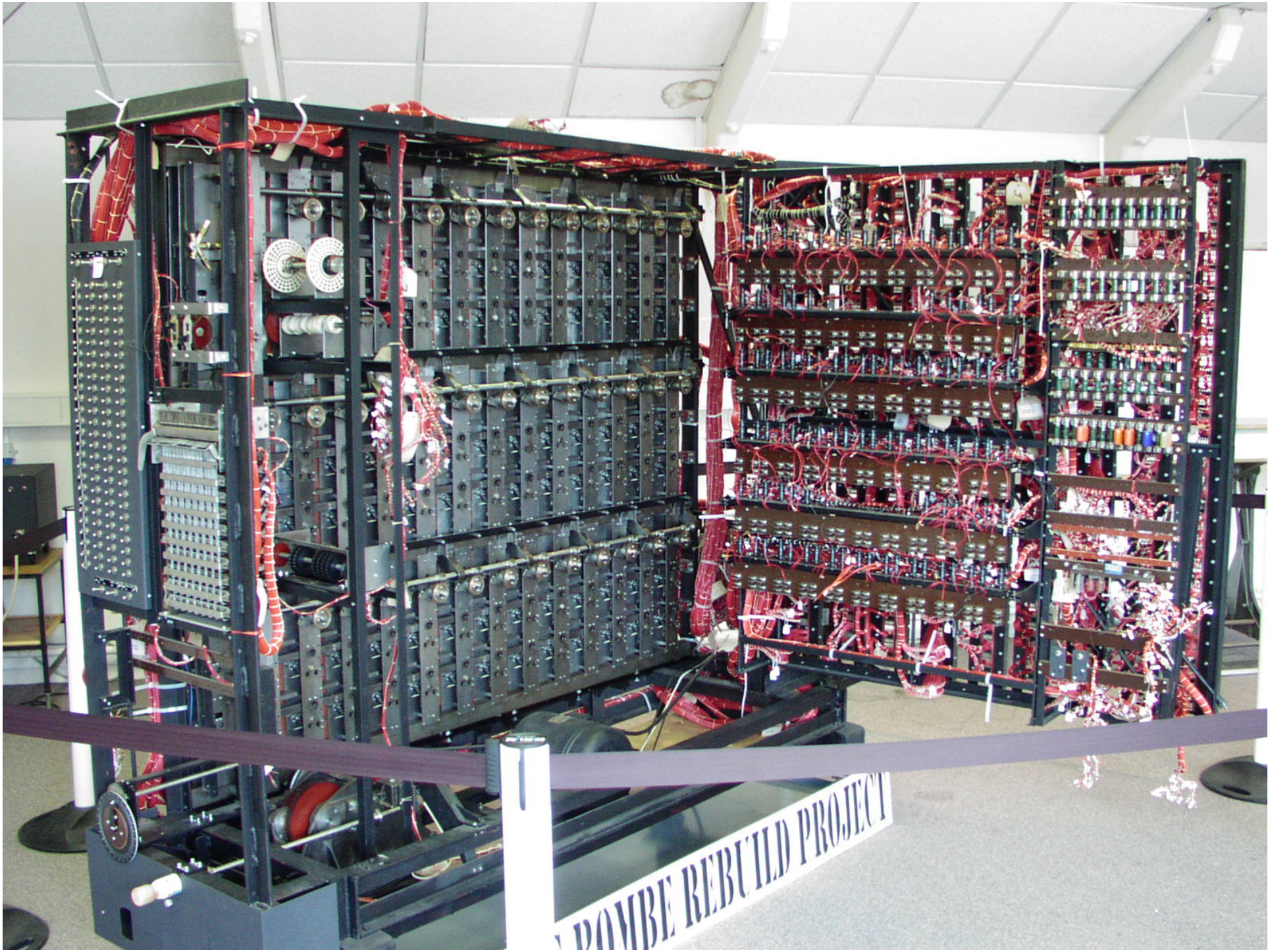
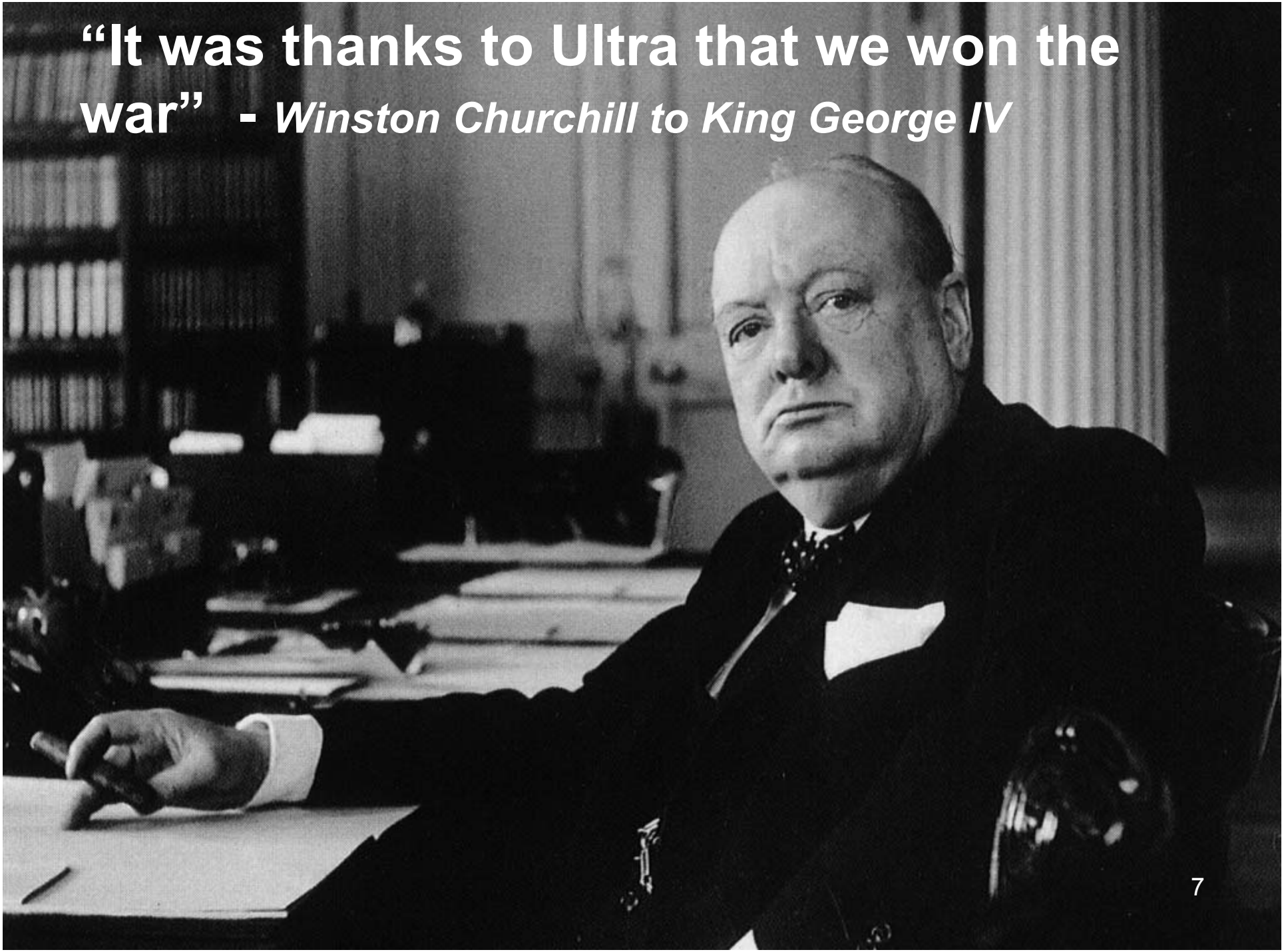
Asymmetric Cryptography

"Information security is becoming a big problem here. Do you still have my Captain Crunch decoder ring, Ma?"

But First…


ROMBE REBUILD PROJECT


“It was thanks to Ultra that we won the war” - *Winston Churchill to King George IV*

Enigma

- http://www.youtube.com/watch?v=elYw4Ve4F-I

Symmetric vs. Asymmetric Ciphers

- In **symmetric ciphers**, the encryption and decryption keys are the same. Both the sender and receiver know the key.

- In **asymmetric ciphers**, the encryption and decryption keys are different. The sender knows only the encryption key and the recipient knows only the decryption key.

Asymmetric Encryption Keys

- In asymmetric cryptography, each user gets a *keypair* consisting of:
  - Public key (freely distributed)
  - Private key (kept secret)

- This allows for greatly enhanced scalability…

Number of Keys Required

Users	Symmetric Keys	Asymmetric Keys
2	1	2
3	3	6
4	6	8
5	10	10
10	45	20
100	4,950	200
20,000	199,990,000	40,000
Formula:	$\frac{n(n-1)}{2}$	**2n**

Cryptographic Goals Revisited

Feature	Symmetric	Asymmetric
Confidentiality	Yes	Yes
Integrity	Yes (but limited)	Yes
Authentication	Yes (but limited)	Yes, Digital Certificates
Non-repudiation	No	Yes, Digital Signatures

What's the Deal?

- Why would you want to use symmetric cryptography at all?
- Speed
  - Symmetric cryptography encrypts and decrypts *much* faster than asymmetric
  - Asymmetric cryptography often used to exchange a one-time-use symmetric key

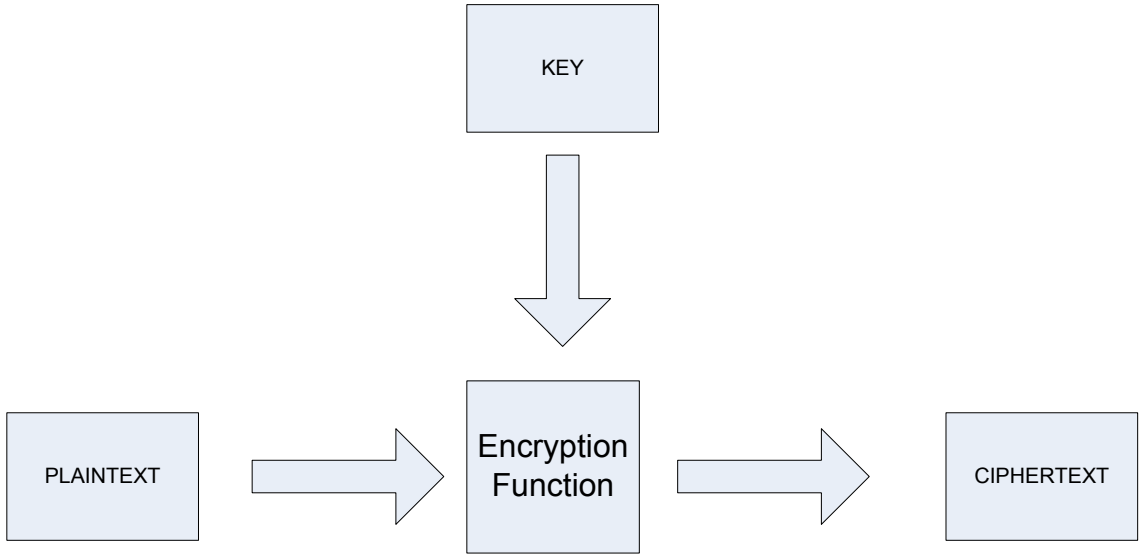
Encrypting Messages

- Remember that each participant has a pair of keys: public and private
  - Alice's keys are $K_{Alice,public}$ and $K_{Alice,private}$
  - Bob's keys are $K_{Bob,public}$ and $K_{Bob,private}$

  - Basic principle of asymmetric cryptography: any message encrypted with one key from a pair may only be decrypted with the other key from the same pair.

Encrypting Messages

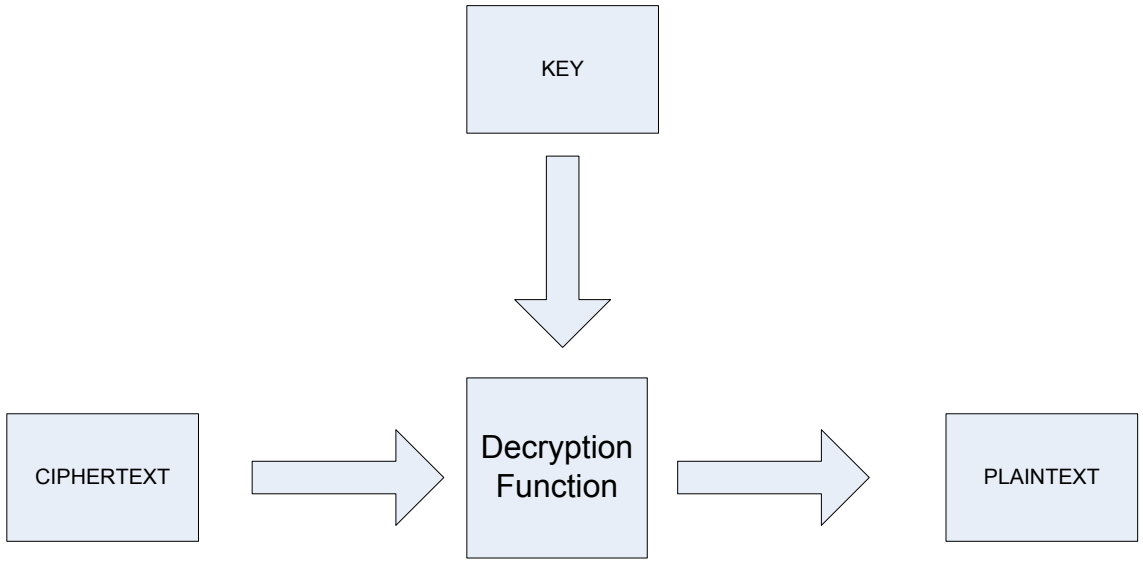
- Suppose that Alice wants to send an encrypted message to Bob…

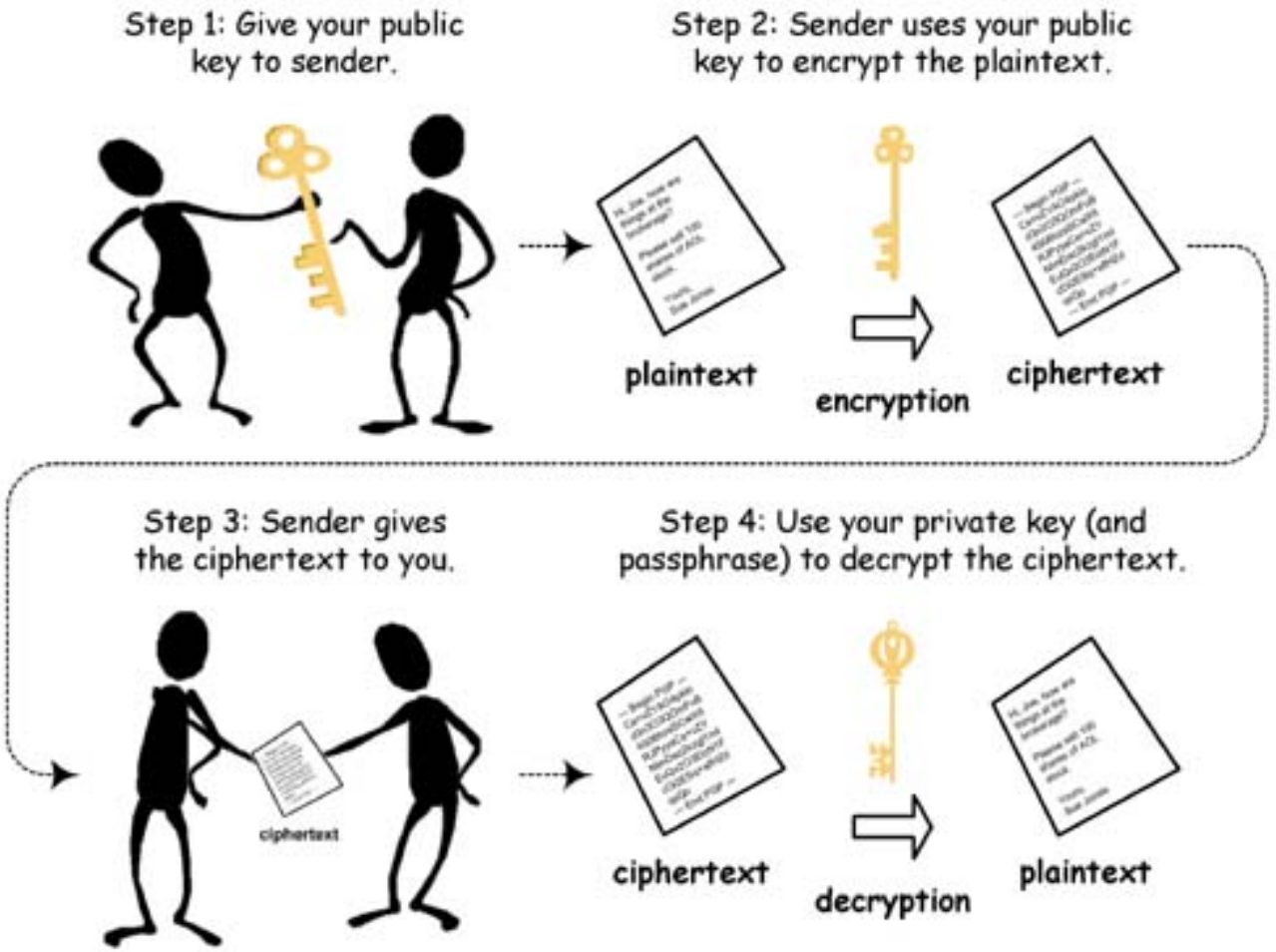


- What key does she use?

Decrypting Messages

- When Bob receives the message, what key does he use to decrypt it?





Source: Nicholas Davis, UW Madison

A Basic Example

- Imagine an asymmetric algorithm:
  - $E(P) = k_{pub} * P = C$
  - $D(C) = k_{priv} * C = P$
- A keypair might be:
  - $k_{pub} = 5$, $k_{priv} = 1/5$
- Encrypt the message P=25
- In the real world, the relationship between public and private keys is *far* more complex

RSA Encryption

Key Generation	
Select p, q	p and q both prime
Calculate n	$n = p \times q$
Select integer d	$gcd(\phi(n), d) = 1;\ 1 < d < \phi(n)$
Calculate e	$e = d^{-1} \bmod \phi(n)$
Public Key	$KU = \{e, n\}$
Private Key	$KR = \{d, n\}$

Encryption
Plaintext: $M < n$
Ciphertext: $C = M^e \pmod{n}$

Decryption
Ciphertext: C
Plaintext: $M = C^d \pmod{n}$

Source: Athar Mahboob

Digital Signatures

- Asymmetric algorithms can leverage their basic properties to provide non-repudiation.

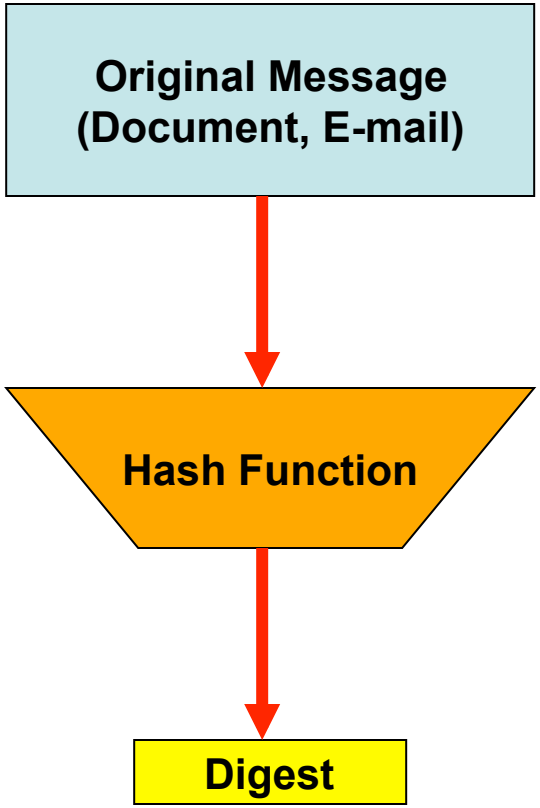
- Who can decrypt a message that you encrypt with your private key?

Hash Functions

- One-way functions that map a variable-length input to a unique, fixed-length output (the message digest)
  - It is incredibly difficult to find two messages with the same digest
  - It is impossible to determine the original message from the digest

Using a Hash Function

- Common hash functions include:
  - MD5
  - SHA-1
- Notice, there is no key used with the hash function.
  - Why?



Source: C.C. Cheung

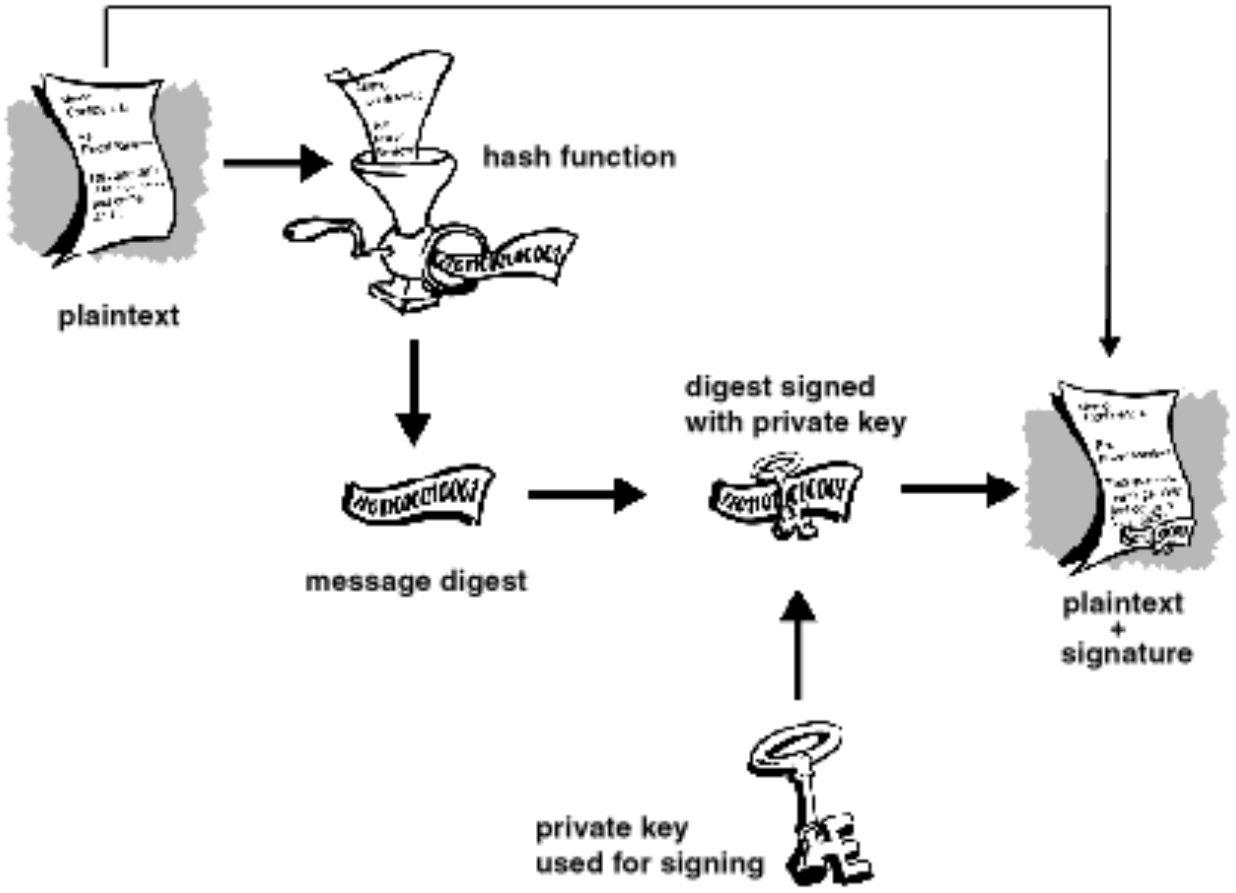
Let's Try It!

- Message: "Cheer, cheer for old Notre Dame"
  - MD5 hash: "7f85aecd277af0eec8a67aa67011db01"
- When hashing, case, punctuation and spacing are all significant!
  - Leave out the comma and the hash becomes: "fdeaed02761a2304b3de6c4ee2204bda"
- http://pajhome.org.uk/crypt/md5/

Digital Signatures

- Digital signatures use hash functions and asymmetric cryptography to enforce non-repudiation
- Useful for proving the authenticity of e-mail messages, documents, etc.
- Allows any third party to definitively confirm that a message came from a specific sender

Creating a Digital Signature

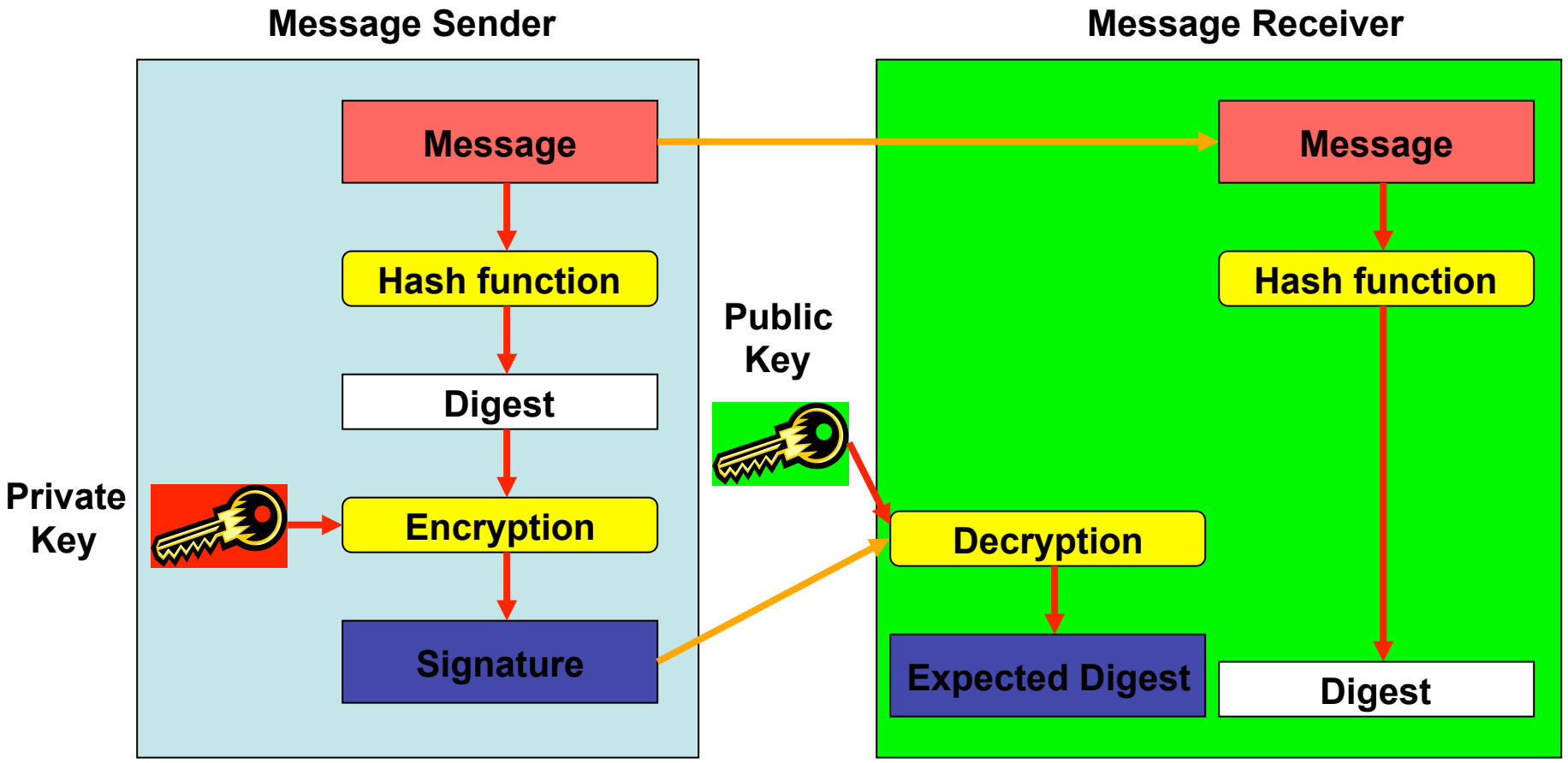


Source: http://www.pgpi.org/doc/pgpintro/

In Other Words…

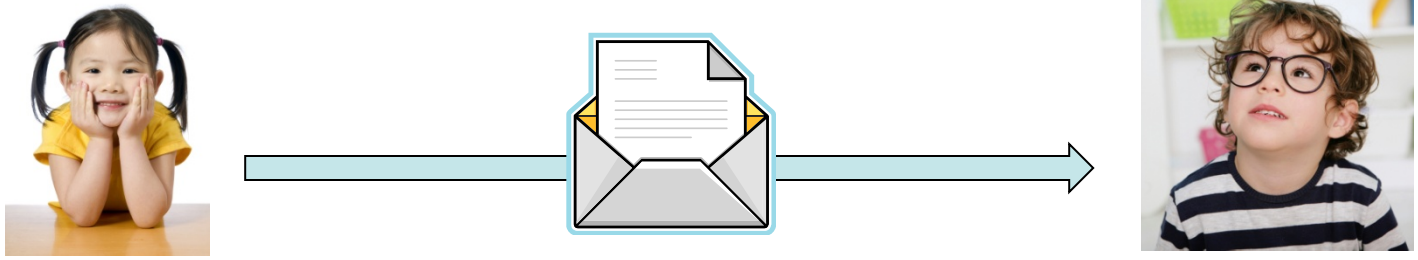
- Creating a digital signature:
  1. Generate a message digest using hash function (like SHA)
  2. Encrypt it with your private key
  3. Attach it to the message
- Verifying a digital signature:
  1. Decrypt the digital signature with the sender's public key
  2. Generate a message digest from the original message
  3. Compare the two, match=non-repudiation

The Entire Process



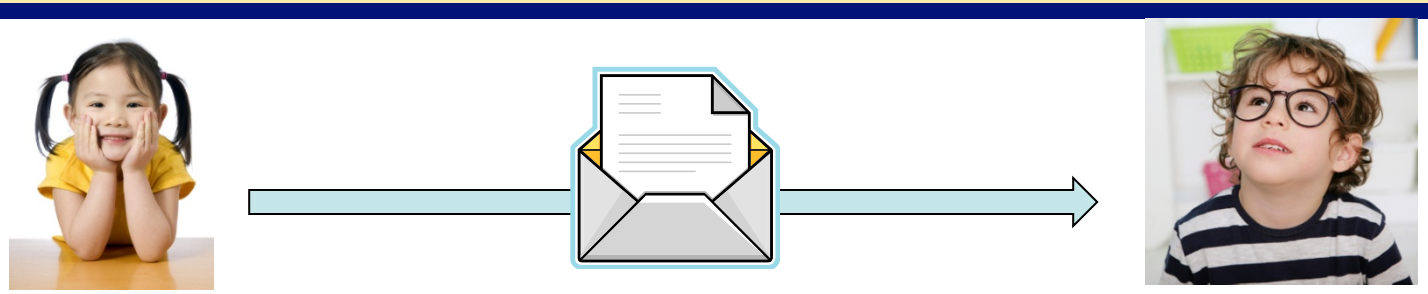
Source: C.C. Cheung

Let's Review…



- Alice wants to send a message to Bob using symmetric cryptography
  - What key does Alice use to encrypt it?
  - What key does Bob use to decrypt it?
  - If Alice wants to sign the message, what key does she use to create the signature?

Let's Review…



- Alice wants to send a message to Bob using asymmetric cryptography
  - What key does Alice use to encrypt it?
  - What key does Bob use to decrypt it?
  - If Alice wants to sign the message, what key does she use to create the signature?
  - What key does Bob use to verify the signature?

Key Exchange

- We talked earlier about the difficulty of exchanging symmetric keys
- Asymmetric cryptography makes this easier, but…
- How do you know the public key you receive is legitimate?

Digital Certificates

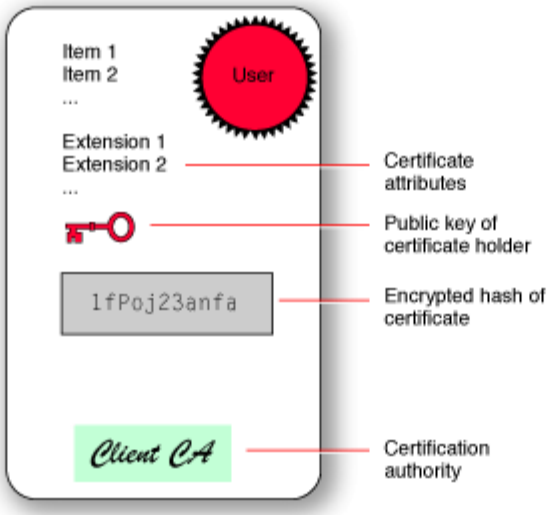
- Digital Certificates use asymmetric cryptography to facilitate the secure exchange of public keys.

- Rely upon the use of trusted Certificate Authorities
  - Certificate Authorities responsible for vouching for identity of certificate “subjects”.
  - Usually used for servers, can also be used by individuals.
  - Organization proves its identity to the CA and the CA provides a signed certificate that can be used to prove identity to others.

- To a CA, trust is essential!

What's in a Digital Certificate?

- Name of the certificate subject
- Subject's public key
- Name of the CA
- Serial number
- Signature algorithm
- Validity period
- CA's digital signature



Source: Apple Computer

Using Certificates in HTTPS

- HTTPS uses digital certificates to ensure secure web communications
- It supplements the standard HTTP protocol with SSL encryption
  1. You access a secure site using your web browser
  2. Your browser retrieves the site certificate and verifies it
     - What does a certificate error mean?
  3. Your browser then chooses a symmetric key, encrypts it with the server's public key and sends it to the server
     - Why don't they just communicate using the server's public key?
  4. Everything from that point forward is encrypted with the symmetric key


DigiNotar
Internet Trust Services

Let's look at a real certificate…