Network Security

Secure communication

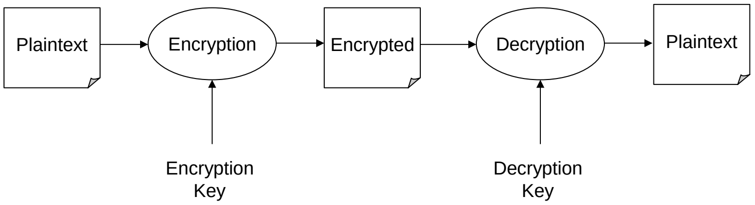
- What does it mean to communicate “securely”?
  - Secrecy: Only the sender and the intended receiver should be able to understand the message
  - Authentication: Both sender and receiver need to be able to confirm the identity of the other.
  - Message integrity: Need to ensure that the message is not altered maliciously or by accident

The University Of Alabama in Huntsville Computer Science

Encryption

cs570

- Implementing secrecy generally implies some form of encryption

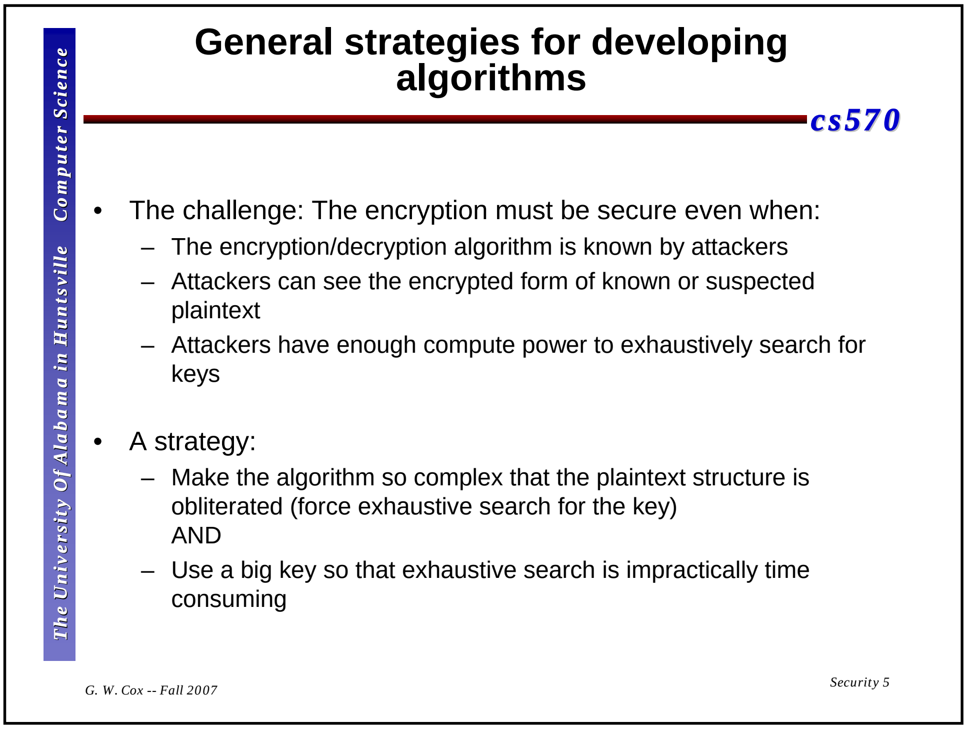


The University Of Alabama in Huntsville Computer Science

Classes of cryptographic algorithms

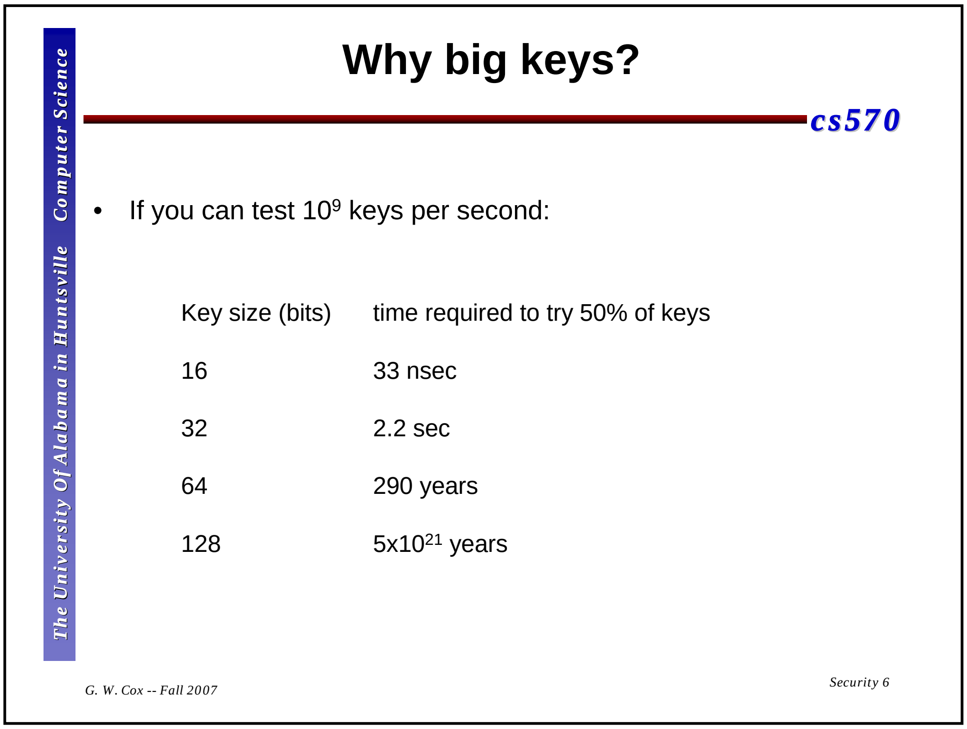
cs570

- Secret Key (AKA “Symmetric Key”)
  - Encryption key is the same as Decryption key
  - Must keep key secret --
  - Ex: DES
- Public Key
  - Encryption key is public, Decryption key is secret
  - Ex: RSA



General strategies for developing algorithms

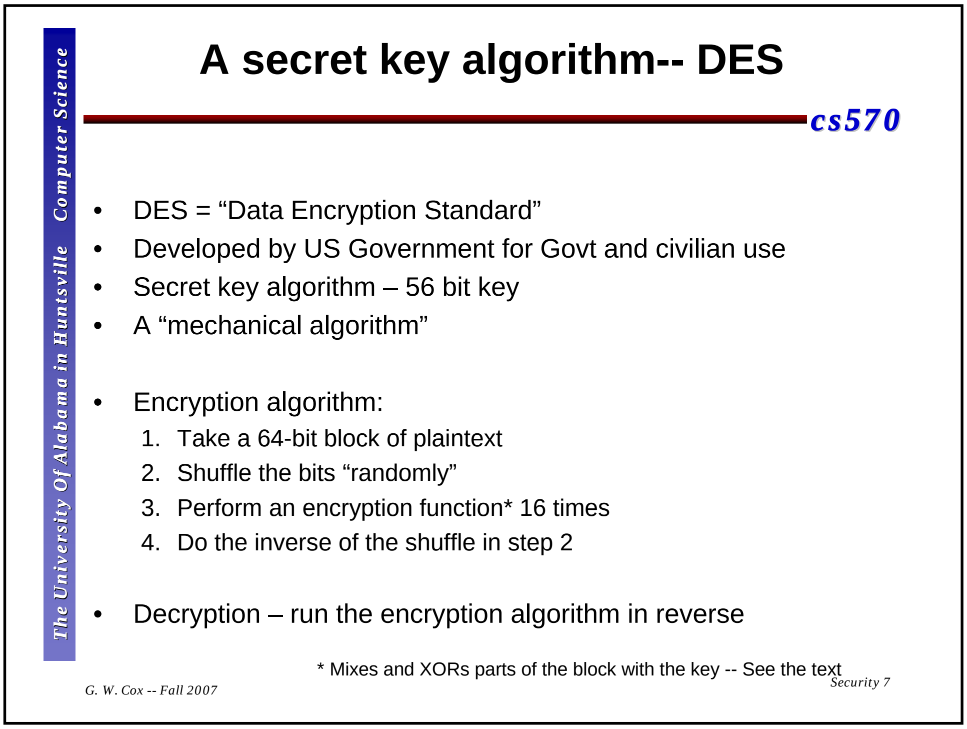
- The challenge: The encryption must be secure even when:
  - The encryption/decryption algorithm is known by attackers
  - Attackers can see the encrypted form of known or suspected plaintext
  - Attackers have enough compute power to exhaustively search for keys
- A strategy:
  - Make the algorithm so complex that the plaintext structure is obliterated (force exhaustive search for the key)
    AND
  - Use a big key so that exhaustive search is impractically time consuming



Why big keys?

- If you can test 10^9 keys per second:

Key size (bits)	time required to try 50% of keys
16	33 nsec
32	2.2 sec
64	290 years
128	$5x10^{21}$ years



The University Of Alabama in Huntsville Computer Science

A secret key algorithm-- DES

cs570

- DES = “Data Encryption Standard”
- Developed by US Government for Govt and civilian use
- Secret key algorithm – 56 bit key
- A “mechanical algorithm”

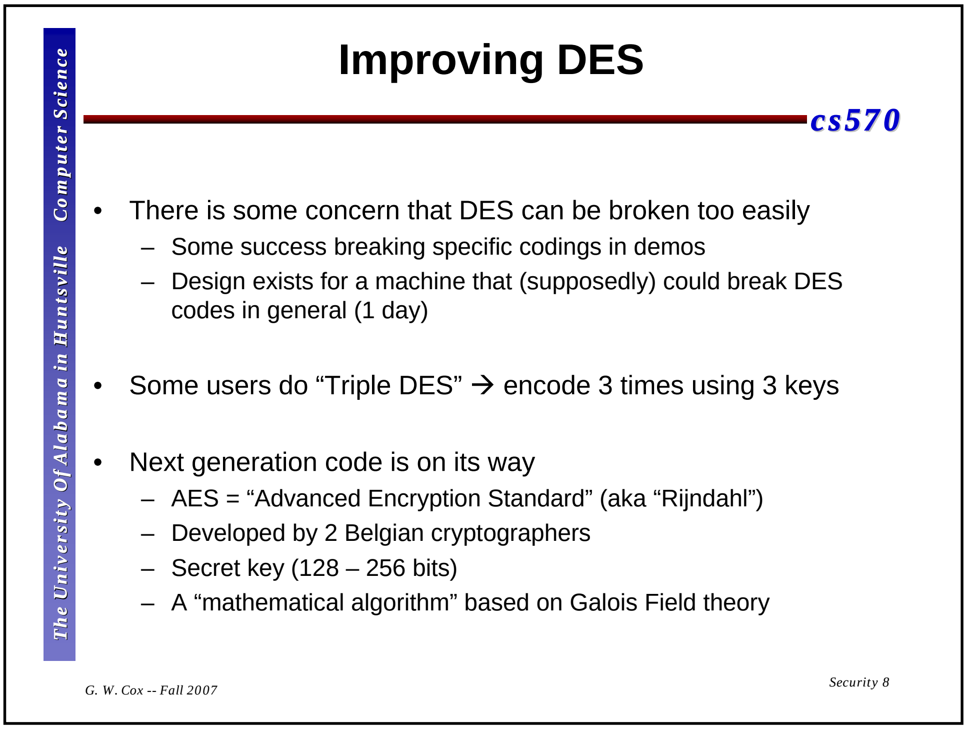
- Encryption algorithm:
  1. Take a 64-bit block of plaintext
  2. Shuffle the bits “randomly”
  3. Perform an encryption function* 16 times
  4. Do the inverse of the shuffle in step 2

- Decryption – run the encryption algorithm in reverse

* Mixes and XORs parts of the block with the key -- See the text

G. W. Cox -- Fall 2007

Security 7



The University Of Alabama in Huntsville Computer Science

Improving DES

cs570

- There is some concern that DES can be broken too easily
  - Some success breaking specific codings in demos
  - Design exists for a machine that (supposedly) could break DES codes in general (1 day)

- Some users do “Triple DES” → encode 3 times using 3 keys

- Next generation code is on its way
  - AES = “Advanced Encryption Standard” (aka “Rijndahl”)
  - Developed by 2 Belgian cryptographers
  - Secret key (128 – 256 bits)
  - A “mathematical algorithm” based on Galois Field theory

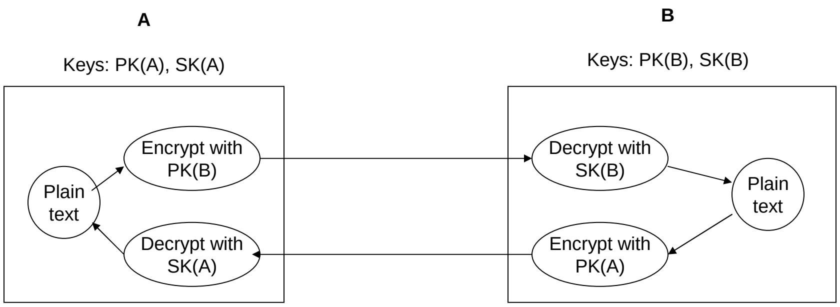
G. W. Cox -- Fall 2007

Security 8

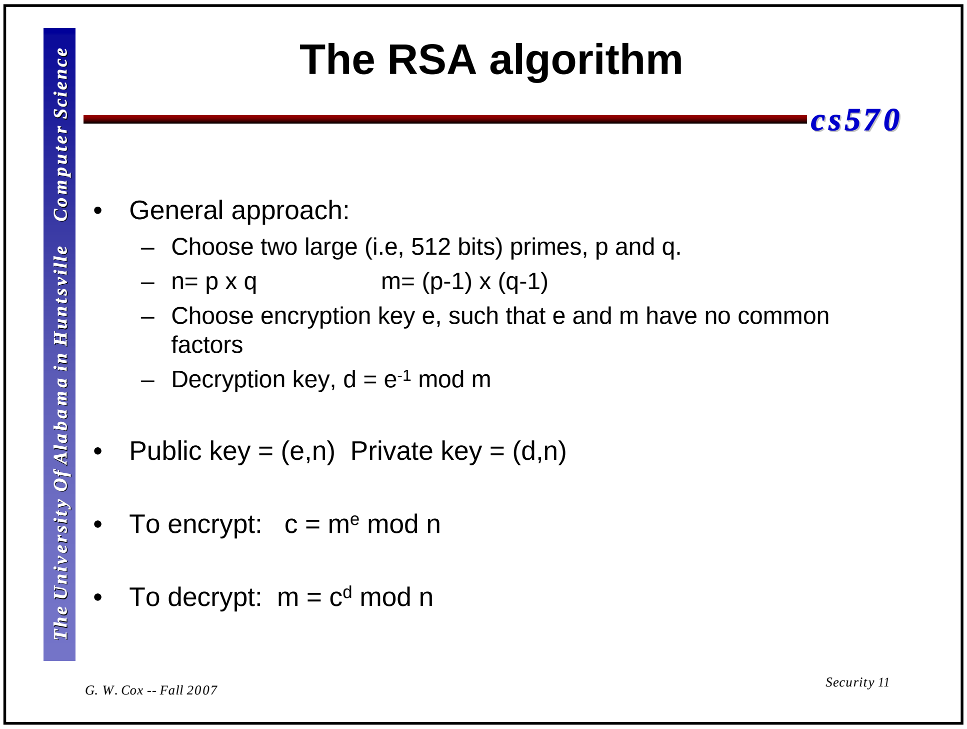
A public key algorithm -- RSA

- RSA = “Rivest, Shamir, and Adleman” (developers)
- 1024-2048 bit keys (at least)
- Very strong
  - Breaking requires factorization of huge numbers (NP time)
  - A P-time algorithm exists for a quantum computer (which doesn’t exist –yet)

How public key systems work



Note: PK(x) cannot decrypt a message encrypted with PK(x)



The RSA algorithm

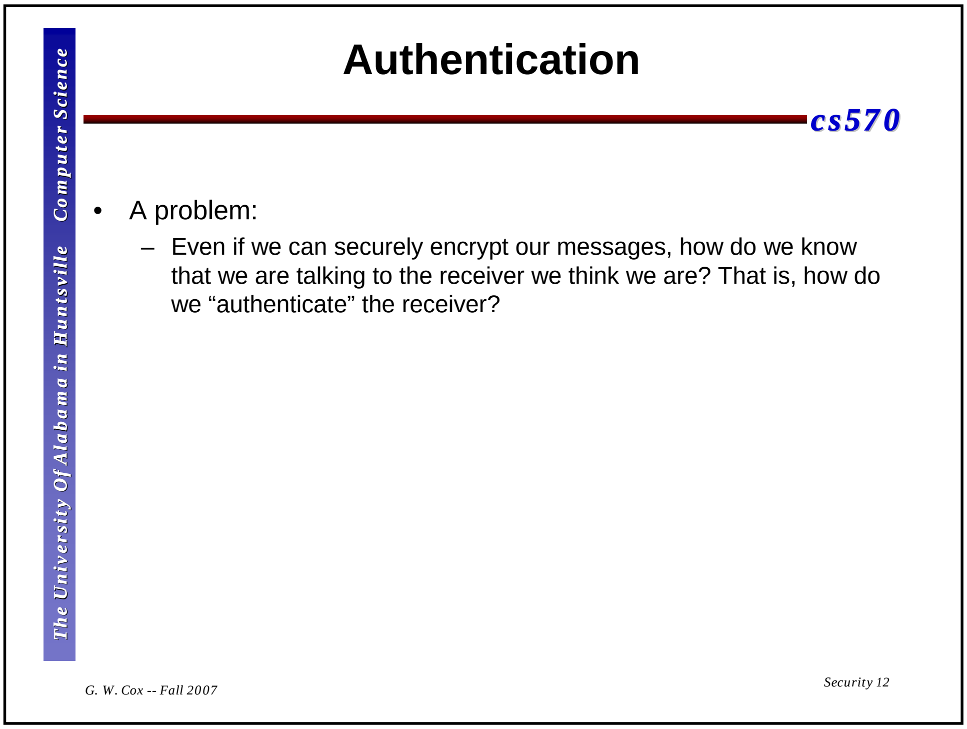
cs570

The University Of Alabama in Huntsville Computer Science

- General approach:
  - Choose two large (i.e, 512 bits) primes, p and q.
  - n= p x q m= (p-1) x (q-1)
  - Choose encryption key e, such that e and m have no common factors
  - Decryption key, $d = e^{-1} \bmod m$
- Public key = (e,n) Private key = (d,n)
- To encrypt: $c = m^{e} \bmod n$
- To decrypt: $m = c^{d} \bmod n$

G. W. Cox -- Fall 2007

Security 11



Authentication

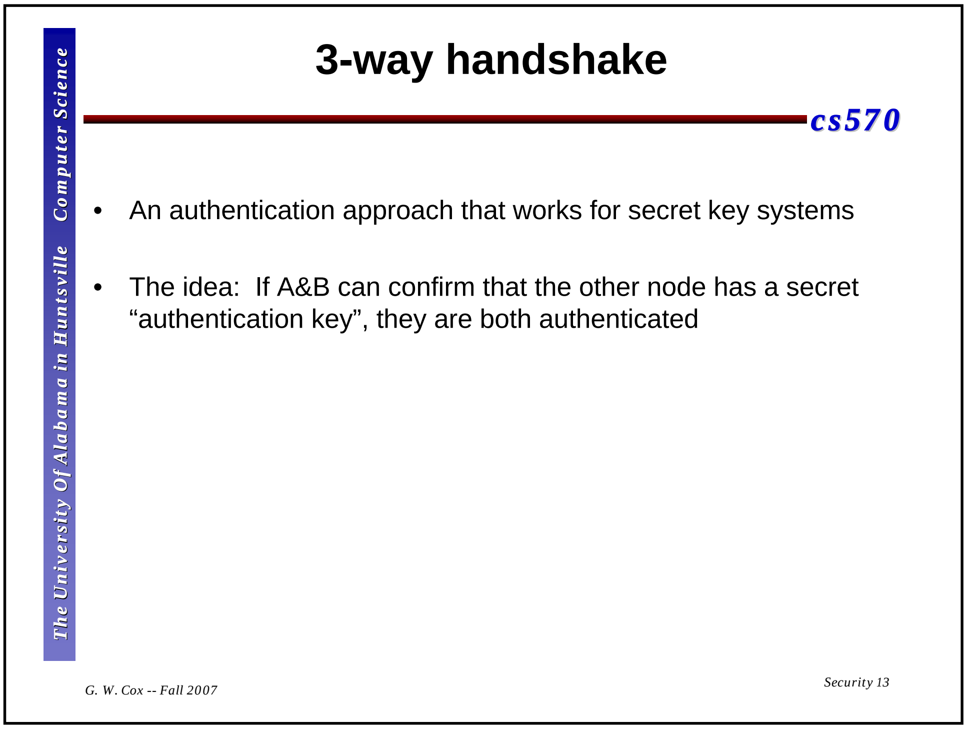
cs570

The University Of Alabama in Huntsville Computer Science

- A problem:
  - Even if we can securely encrypt our messages, how do we know that we are talking to the receiver we think we are? That is, how do we “authenticate” the receiver?

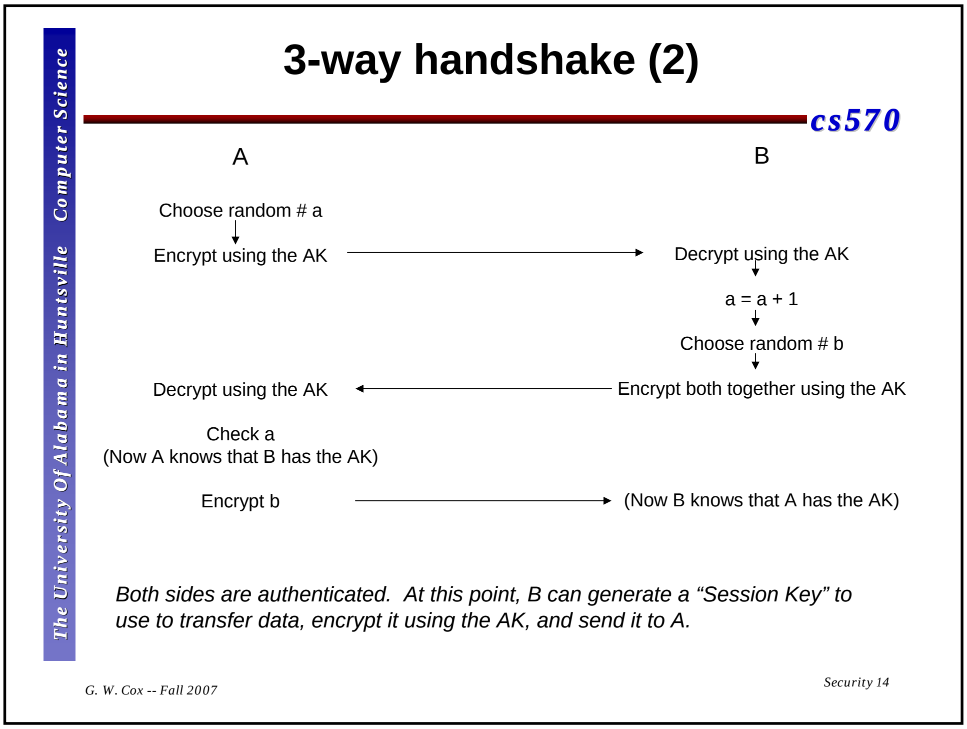
G. W. Cox -- Fall 2007

Security 12



3-way handshake

- An authentication approach that works for secret key systems
- The idea: If A&B can confirm that the other node has a secret “authentication key”, they are both authenticated



3-way handshake (2)

A

Choose random # a

Encrypt using the AK

B

Decrypt using the AK

a = a + 1

Choose random # b

Encrypt both together using the AK

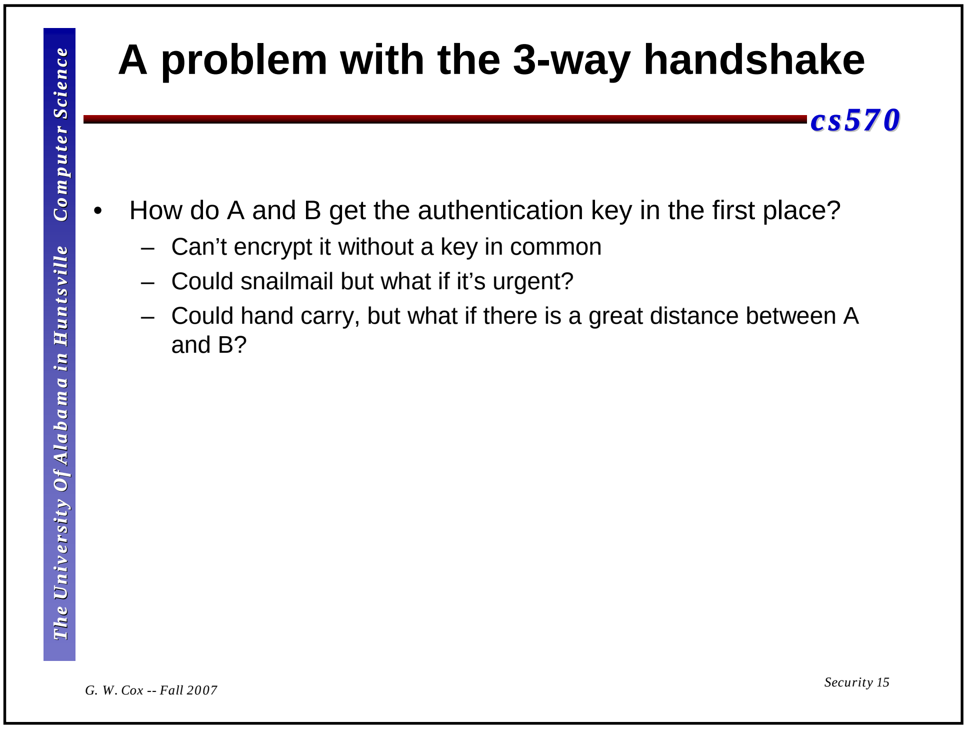
Decrypt using the AK

Check a
(Now A knows that B has the AK)

Encrypt b

(Now B knows that A has the AK)

Both sides are authenticated. At this point, B can generate a “Session Key” to use to transfer data, encrypt it using the AK, and send it to A.



The University Of Alabama in Huntsville Computer Science

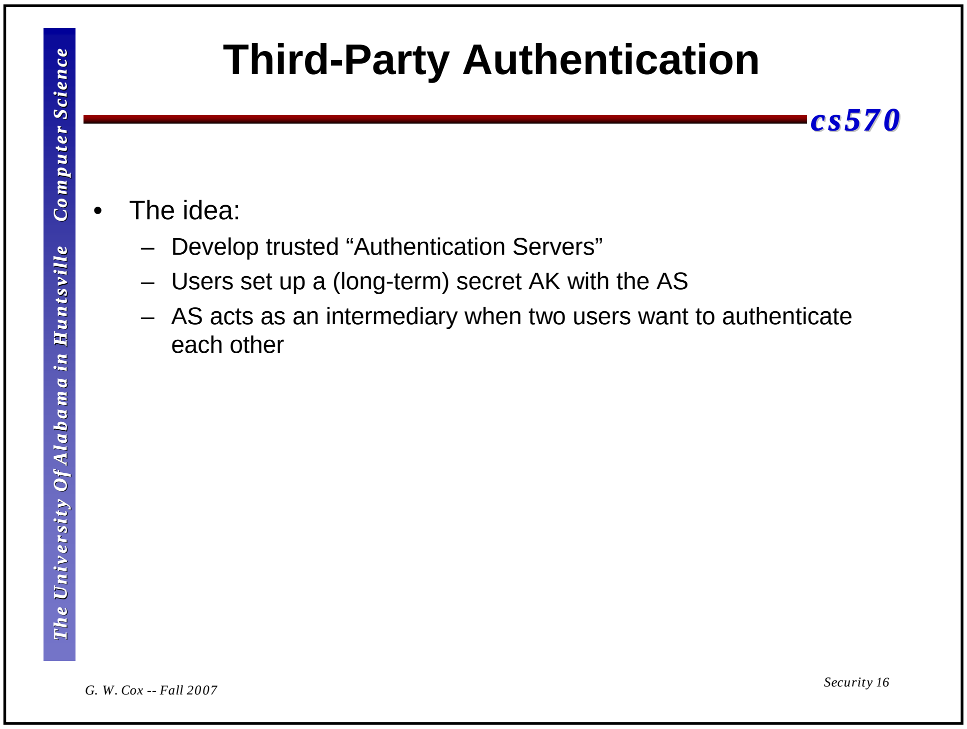
A problem with the 3-way handshake

cs570

- How do A and B get the authentication key in the first place?
  - Can’t encrypt it without a key in common
  - Could snailmail but what if it’s urgent?
  - Could hand carry, but what if there is a great distance between A and B?

G. W. Cox -- Fall 2007

Security 15



The University Of Alabama in Huntsville Computer Science

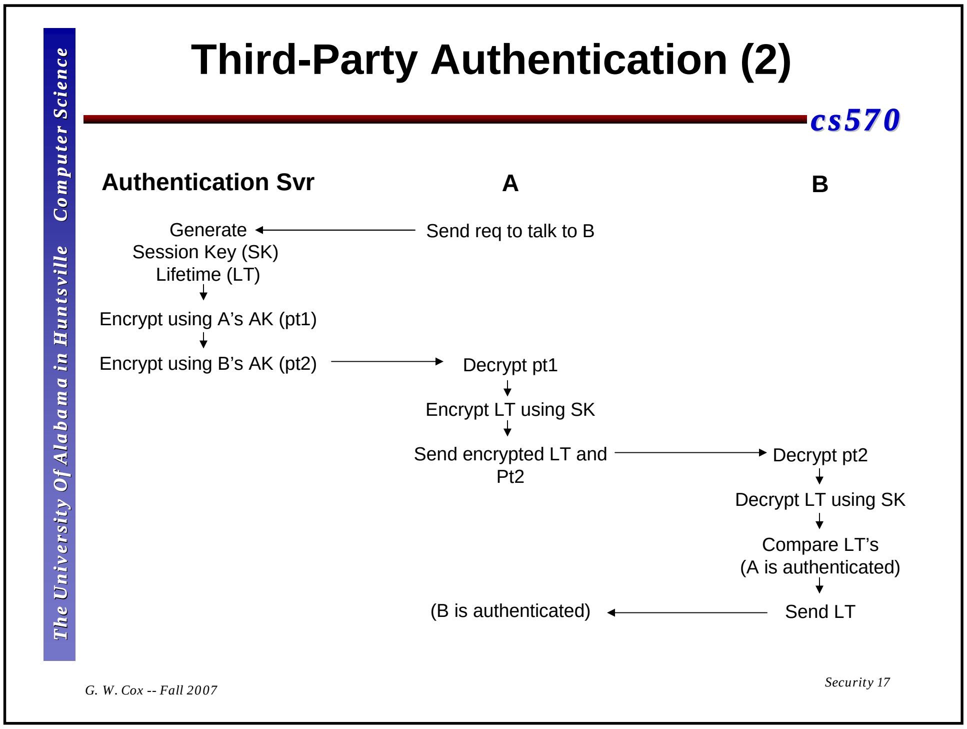
Third-Party Authentication

cs570

- The idea:
  - Develop trusted “Authentication Servers”
  - Users set up a (long-term) secret AK with the AS
  - AS acts as an intermediary when two users want to authenticate each other

G. W. Cox -- Fall 2007

Security 16



The University Of Alabama in Huntsville Computer Science

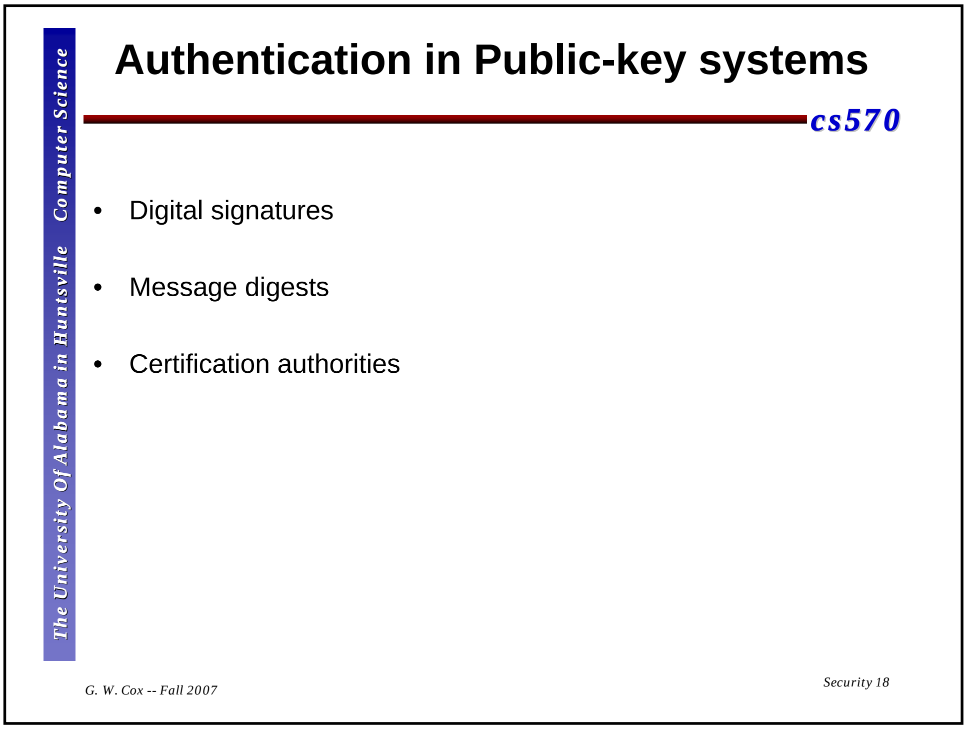
Third-Party Authentication (2)

cs570

Authentication Svr	A	B
Generate Session Key (SK) Lifetime (LT)	Send req to talk to B	
Encrypt using A's AK (pt1)		
Encrypt using B's AK (pt2)	Decrypt pt1	
	Encrypt LT using SK	
	Send encrypted LT and Pt2	Decrypt pt2
		Decrypt LT using SK
		Compare LT's (A is authenticated)
	(B is authenticated)	Send LT

G. W. Cox -- Fall 2007

Security 17



The University Of Alabama in Huntsville Computer Science

Authentication in Public-key systems

cs570

- Digital signatures
- Message digests
- Certification authorities

G. W. Cox -- Fall 2007

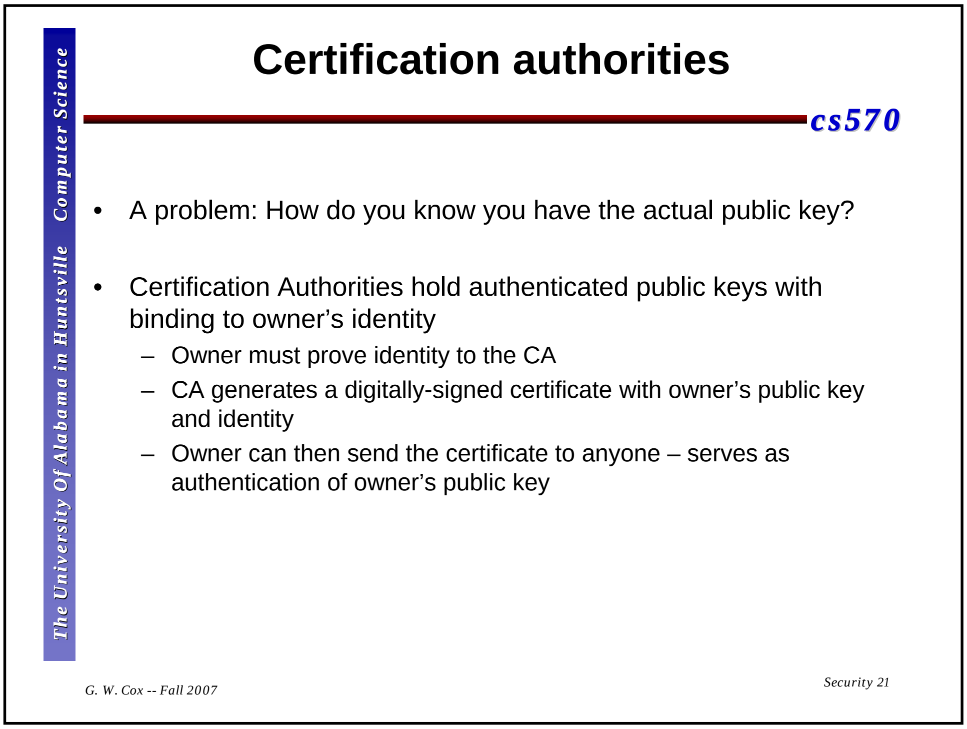
Security 18

Digital signatures

- Used to authenticate that something (e.g, a document, email) comes from you (Public key systems, only) while preserving secrecy
- Based on the fact that in most public key systems, you can equally well encrypt with the secret key, decrypt with the public one
- To send a signed message from A to B
  - A encrypts message using A's secret key
  - Then A encrypts result using B's public key (so no-one but B can read it)
  - B decrypts outer level using B's secret key
  - Then B decrypts the inner level using A's public key (since no-one else has A's secret key, this proves that the message came from A)

Message digests

- Pure authentication of a document – no security
- The idea:
  - From the plaintext, calculate a number ("hash code") that is practically unique to this particular plaintext.
  - Encrypt using the recipient's public key and send with the plaintext (since so little is encrypted, this is much faster than encrypting the entire document)

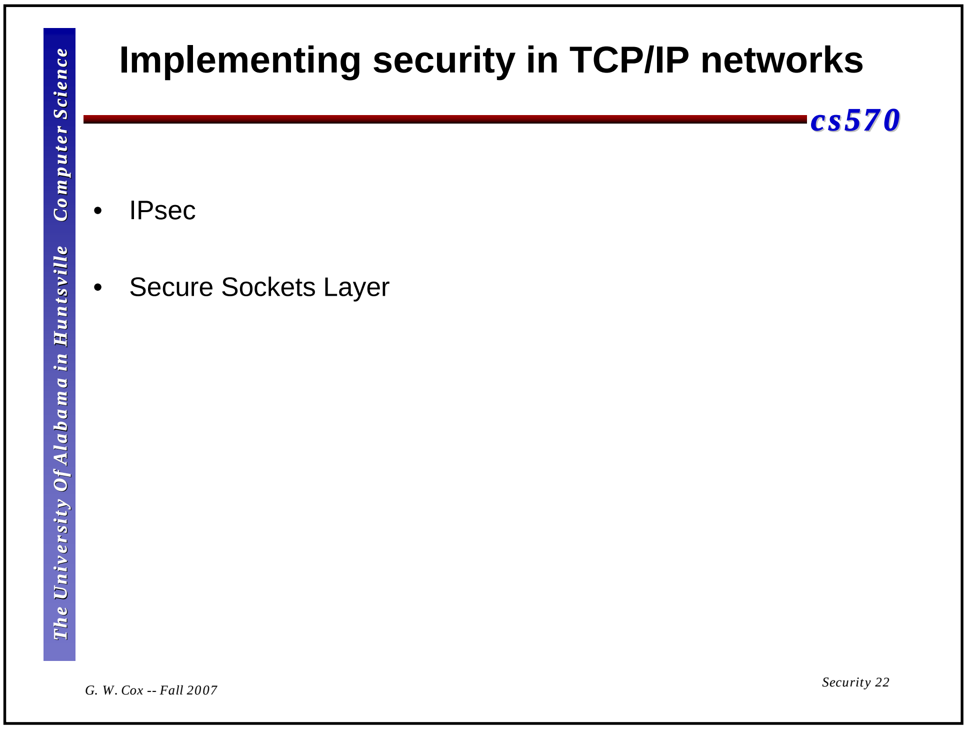


The University Of Alabama in Huntsville Computer Science

Certification authorities

cs570

- A problem: How do you know you have the actual public key?
- Certification Authorities hold authenticated public keys with binding to owner's identity
  - Owner must prove identity to the CA
  - CA generates a digitally-signed certificate with owner's public key and identity
  - Owner can then send the certificate to anyone – serves as authentication of owner's public key

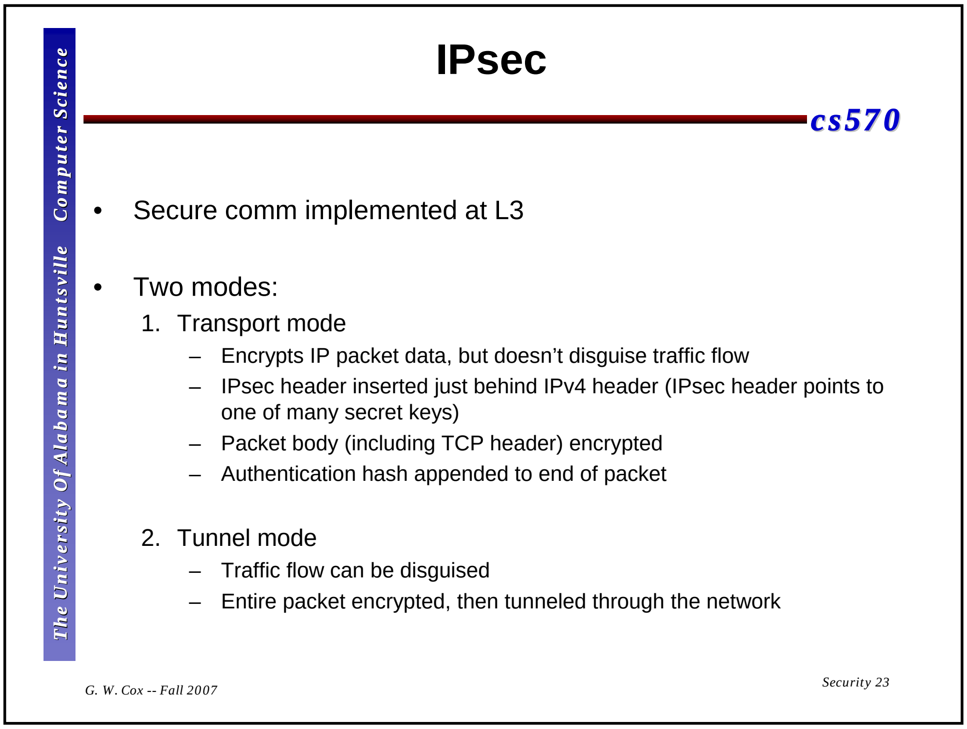


The University Of Alabama in Huntsville Computer Science

Implementing security in TCP/IP networks

cs570

- IPsec
- Secure Sockets Layer



The University Of Alabama in Huntsville Computer Science

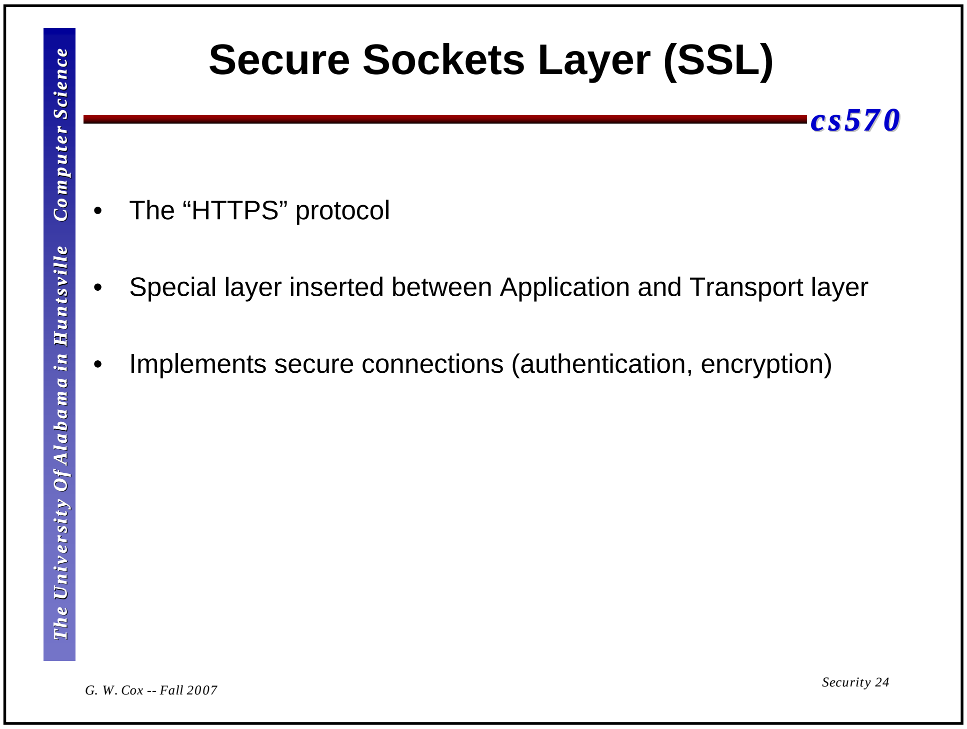
IPsec

cs570

- Secure comm implemented at L3
- Two modes:
  1. Transport mode
     - Encrypts IP packet data, but doesn't disguise traffic flow
     - IPsec header inserted just behind IPv4 header (IPsec header points to one of many secret keys)
     - Packet body (including TCP header) encrypted
     - Authentication hash appended to end of packet
  2. Tunnel mode
     - Traffic flow can be disguised
     - Entire packet encrypted, then tunneled through the network

G. W. Cox -- Fall 2007

Security 23



The University Of Alabama in Huntsville Computer Science

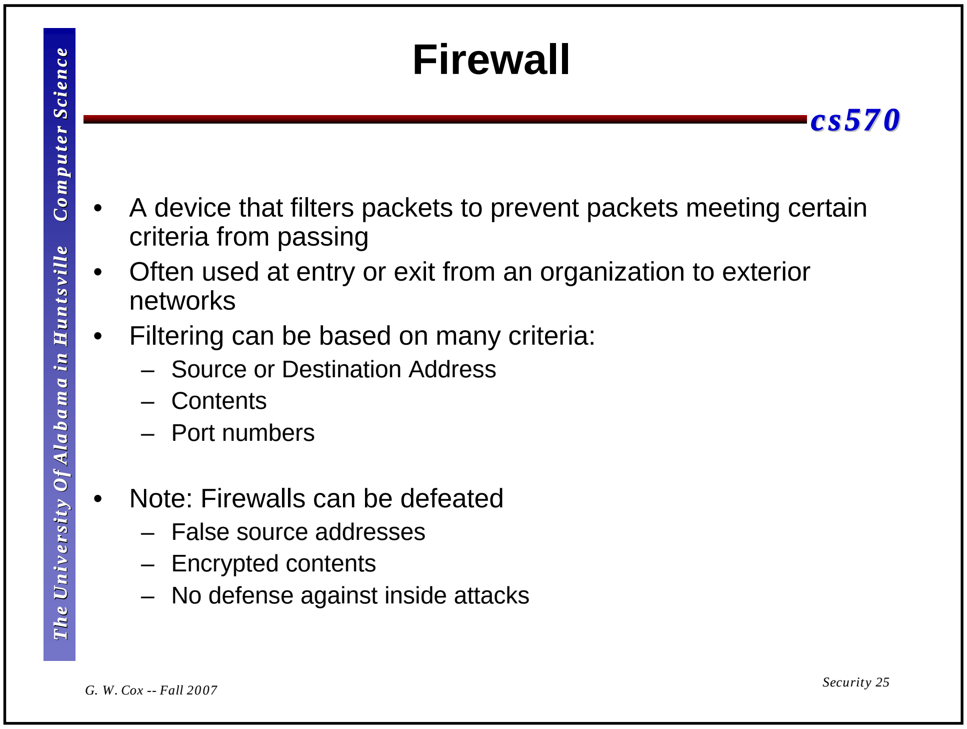
Secure Sockets Layer (SSL)

cs570

- The "HTTPS" protocol
- Special layer inserted between Application and Transport layer
- Implements secure connections (authentication, encryption)

G. W. Cox -- Fall 2007

Security 24



Firewall

- A device that filters packets to prevent packets meeting certain criteria from passing
- Often used at entry or exit from an organization to exterior networks
- Filtering can be based on many criteria:
  - Source or Destination Address
  - Contents
  - Port numbers

- Note: Firewalls can be defeated
  - False source addresses
  - Encrypted contents
  - No defense against inside attacks