Security in Layers and Attack Mitigation & Threat Pragmatics, Cryptography Basics

Fakrul Alam
bdHUB Limited
fakrul@bdhub.com

Acknowledgement

Steven M. Bellovin

https://www.cs.columbia.edu/~smb

Merike Kaeo

merike@doubleshotsecurity.com

Targets

- Many sorts of targets:
  - Network infrastructure
  - Network services
  - Application services
  - User machines

What's at risk?

Network Infrastructure

- Routers (and routing protocols)
- Switches and other network elements
- Links

Links

- Primary risk is wiretapping
- Easily defeated by encryption—but are people using it?
- Most encryption doesn't protect against traffic analysis—but that isn't in everyone's threat model
- Link-layer encryption protects against most traffic analysis, but it has to be done on every vulnerable link

Traffic Analysis

- Looks at *external* characteristics of traffic: who talks to whom, size of messages, etc.
- *Very* valuable to intelligence agencies, police, etc.
  - Who works with whom? Who gives orders to whom?
- Not generally useful for ordinary thieves, though a few sophisticated attackers could use it to find targets

Solutions

- Use VPNs or application-level encryption
- Use link encryption for high-risk links (e.g., WiFi)
- Also use link encryption for access control (especially WiFi)
- Don’t worry about traffic analysis

(Is WiFi Safe?)

- Inside an organization, WiFi+WPA2 Enterprise is generally safe enough without further crypto
  - However, it's harder to trace an infected host that's doing address-spoofing
- For external WiFi, *always* use crypto, preferably VPNs
  - Make sure you do mutual authentication
- There is some residual risk if your VPN doesn't drop unencrypted inbound traffic

Switches and the Like

- Compromised switches can be used for eavesdropping
- Special risk in some situations: reconfigured VLANs
  - VLANs provide good traffic separation between user groups
  - Especially useful against ARP- and MAC-spoofing attackers
- Other danger point: the monitoring port

ARP and MAC Spoofing

- ARP maps the IP address desired to a MAC address
- Switches learn what MAC addresses are on what ports, and route traffic accordingly
- If a malicious host sends out traffic with the wrong MAC address, the switch will send traffic to it
- If a malicious host replies to an ARP query for some other machine, the malicious host will receive the traffic, but this might be noticed

Defenses

- Harden switch access
  - ACLs
  - ssh-only access; no passwords
- Hosts should use crypto and cryptographic authentication

Routers

- Routers can be used for the same sorts of attacks as switches
- Because routers inherently separate different networks, they always defend against certain kinds of address spoofing
  - This makes them targets
- Worse yet, routers can launch *routing protocol attacks*

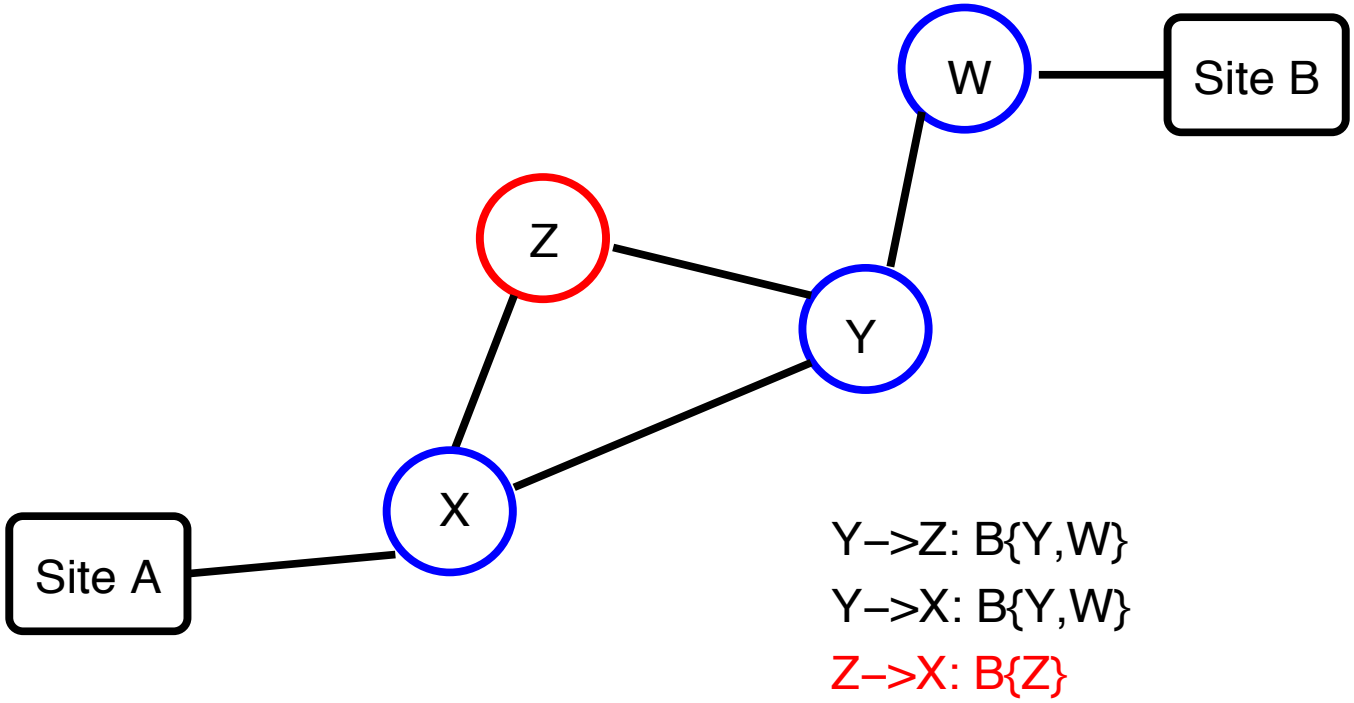
Routing Protocol Attacks: Effects

- Traffic is diverted
  - Attacker can see the traffic and do traffic analysis
  - Attacker can modify packets
  - Attacker can drop packets
  - Attacker can hijack prefixes
- End-to-end crypto can protect the packets' contents, but can't stop traffic analysis or denial of service

Why is Routing Security Different?

- Most security failures are due to buggy code, buggy protocols, or buggy sysadmins
- Routing security problems happen when everything is working right, but some party decides to lie. The problem is a dishonest participant
- Most routers can lie to any routing protocols they speak

A Routing Attack



Z claims that it has a shorter path to B than Y does (1 hop versus 2). X believes Z.

Defending Against Routing Attacks

- Must *know* authoritative owner of prefixes
  - Generally done with a certificate signed by the address space owner
  - Being rolled out today as RPKI
- All routing announcements must be digitally signed
  - Each router needs a route-signing certificate
  - All signatures must be over the full path; signatures are thus *nested*
  - In the IETF process as BGPSEC

Network Services

Certain core services are ubiquitous—and frequently attacked

- DNS
- SMTP
- Assorted local services: file servers, printers, LDAP, and more

These are the means, not the goals of the attackers

DNS

DNS responses are easily spoofed by attackers

- Cache contamination
- Query ID guessing
- Deliberate tinkering by ISPs, nation-states, hotels, etc.

Because responses are cached, client/server authentication can't solve it.

Must have *digitally signed* responses

SMTP

- Historically, a major attack target; principle implementations were very buggy
- Today, the big problem is spam; must keep attackers from spamming your users, and from using you to spread spam
- Secondary issue: separate inside and outside email systems—inside email often has sensitive information

Encrypted Email

- Email messages themselves can be encrypted: useful for end-to-end security
- SMTP can be encrypted, too
  - Not that crucial for site-to-site relaying (but eavesdroppers do exist); *very* important for authenticated email submission
  - Your users *must* authenticate somehow—via IP address if inside; via credentials if roaming—before sending mail through your outbound SMTP server

Local Services

- Rarely directly accessible from the Internet; (ab)used after initial penetration
  - Virus spreading
  - File contents, in targeted attacks
  - Privilege escalation
- Quite often buggy, but there's little choice about running them; they're necessary for scalability and productivity

Application Services

- Data center-resident: deliver services to the outside world
- Obvious example: HTTP
- But—HTTP is generally a front end for a vital database
- A prime target

Targeting Application Services

- Generally exposed to the outside—and you can't firewall them, because they *must* be exposed to the outside
- The server can be used for the bad guys' content: phishing servers, "warez" sites, more
- The database often holds very valuable information, like credit cards
- There are usually connections from these servers back into the corporation

User Machines

Ordinary desktops are targets, too

- Plant keystroke loggers to steal passwords, especially for financial sites
- Turn into bots—bandwidth is what matters
- Turn into spam engines; use machine's privileges (generally based on network location) to send out spam through the authorized SMTP server

Users

- Users make mistakes
  - They click on things they shouldn't
  - They visit dangerous sites
  - They mistake phishing emails for the real thing
  - They don't keep their systems up to date
  - "PEBCAK": Problem Exists Between Chair and Keyboard
- (It's not even their fault; our systems are horribly designed)

Social Engineering

- Try to trick people into doing things they shouldn't
- People *want* to help
  - Walk in the door dressed as a delivery or repair person
  - Call and sound like an insider: "Chris, could you reset my password on server #3 in rack 7? Its connection to the RADIUS server is hung."
- A very different skill than purely technical stuff—but *very* useful

HBGary Federal : 2011/Feb

No.1 SQL Injection to CMS

No.2: Steal Password Hashes

No.3: Crack the hash (password of CEO and COO)

No.4: Password re-use to other services...

No.5: Login to other server by SSH (!)

No.6: Use CVE-2010-3856 (vulnerability in glib) to local exploit to get “root”

No.7: Social engineering to get another info

No.8: Login, local-exploit, “root”.

No.9: The END

How does the Social Engineering Happen ?

From: Greg
To: Jussi
Subject: need to ssh into rootkit
im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ?
thanks

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed

From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
no i dont have the public ip with me at the moment because im ready for a small meeting and im in a rush.
if anything just reset my password to changeme123 and give me public ip and ill ssh in and reset my pw.

How does the Social Engineering Happen ?

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
ok,
it should now accept from anywhere to 47152 as ssh. i am doing
testing so that it works for sure.
your password is changeme123

i am online so just shoot me if you need something.

in europe, but not in finland? :-)

_jussi

From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
if i can squeeze out time maybe we can catch up.. ill be in germany
for a little bit.

anyway I can't ssh into rootkit. you sure the ips still
65.74.181.141?

thanks

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
does it work now?

From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
yes jussi thanks

did you reset the user greg or?

How does the Social Engineering Happen ?

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
nope. your account is named as hoglund

From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
yup im logged in thanks ill email you in a few, im backed up

thanks

Cryptography

Topics To Cover

- Symmetric Keys
- Asymmetric Keys
- Hash Functions
- Encryption
- Signing

Cryptography Is Used For?

- Authentication Protocols
- Data Origin Authentication
- Data Integrity
- Data Confidentiality

Crypto Basics

- Building Blocks
  - Crypto algorithm: specifies the mathematical transformation that is performed on data to encrypt/decrypt
  - Stream cipher: encrypts a digital stream one bit at a time (RC4)
  - Block cipher: transforms data in fixed-size blocks, one block at a time
    - DES (56-bit keys; 64-bit blocksize)
    - AES (128-, 192-, and 256-bit keys; 128-bit blocksize)
- Good Crypto Algorithm Properties
  - Algorithm is NOT proprietary
  - Analyzed by public community to show that there are no serious weaknesses
  - Explicitly designed for encryption

What is a Cryptosystem?

- A cryptosystem is pair of algorithms that take a *key* and convert *plaintext* to *ciphertext* and back.
- Plaintext and ciphertext are arbitrary strings of bits. A key is also a string of bits that *must be kept secret*.
  - Secret key
  - Private key
- Plaintext is what you want to protect; ciphertext should appear to be random gibberish.

Caution

- Cryptography is a very subtle mathematical science
- Even experts make very bad mistakes
- Don't invent your own
  - Example: SSL 3.0 has been around since 1996. It's been through several in-depth, expert reviews. Two new serious flaws have been found in the last five years.
- Don't buy from vendors who say "**our product is more secure because of our proprietary algorithms**"; they're almost always either lying or incompetent

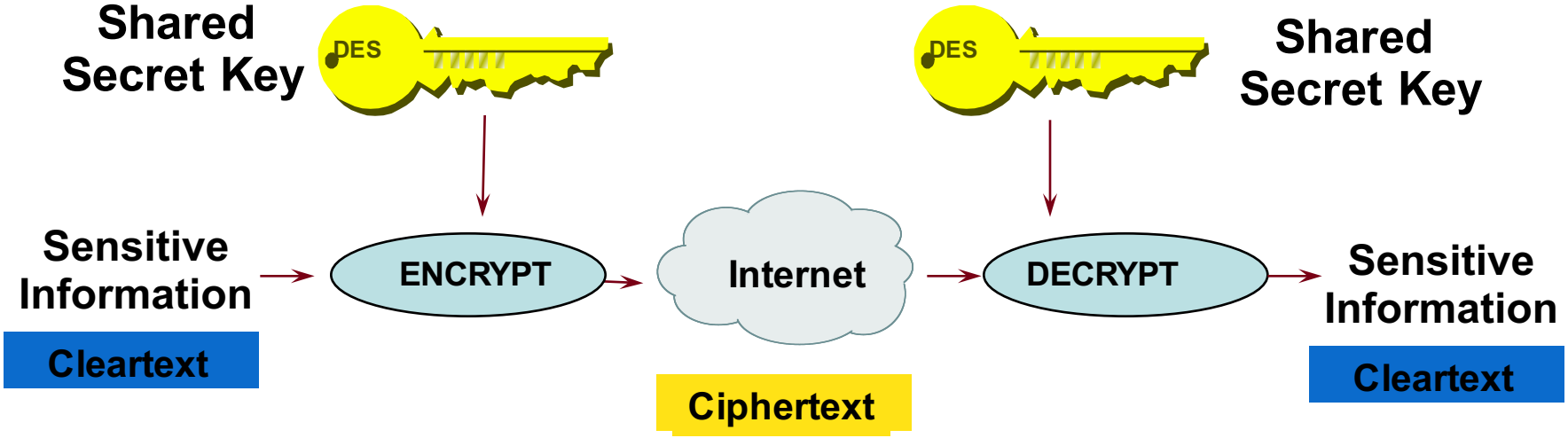
Kerckhoff's Law (1883)

The system must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.

In other words, the security of the system must rest entirely on the secrecy of the key.

Secret Key Encryption

- Two parties share the same secret key
- Problem is securely distributing the key

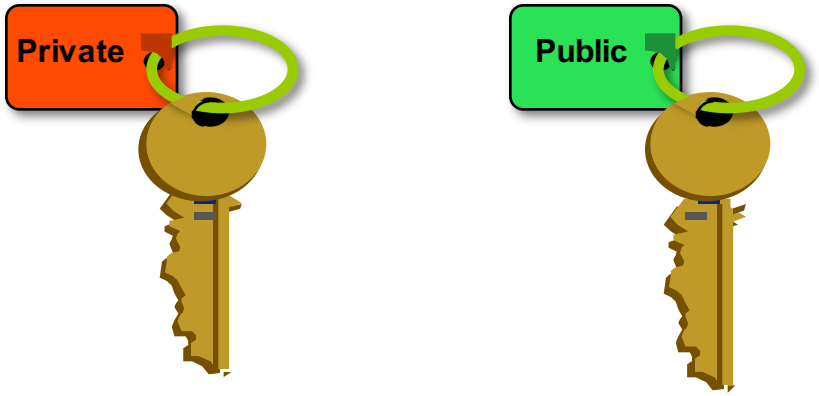


Common Algorithms: DES, 3DES, AES, IDEA

Public Key Encryption

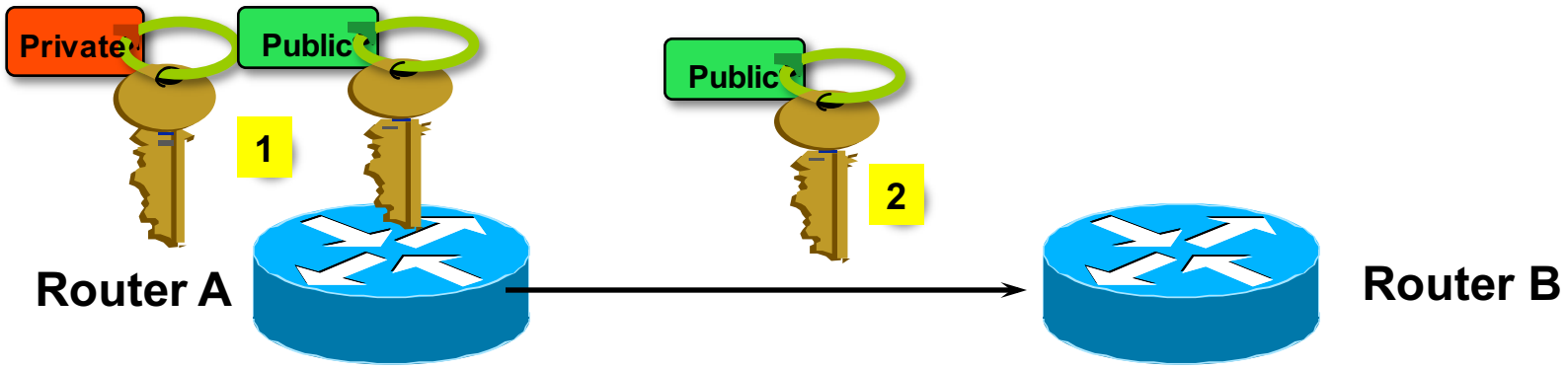
Uses public/private keys

- One key is mathematical inverse of the other
- Private key is only known by owner of the pair
- Public keys are stored in public servers



Common Algorithms: RSA, El Gamal, DSS, ECC

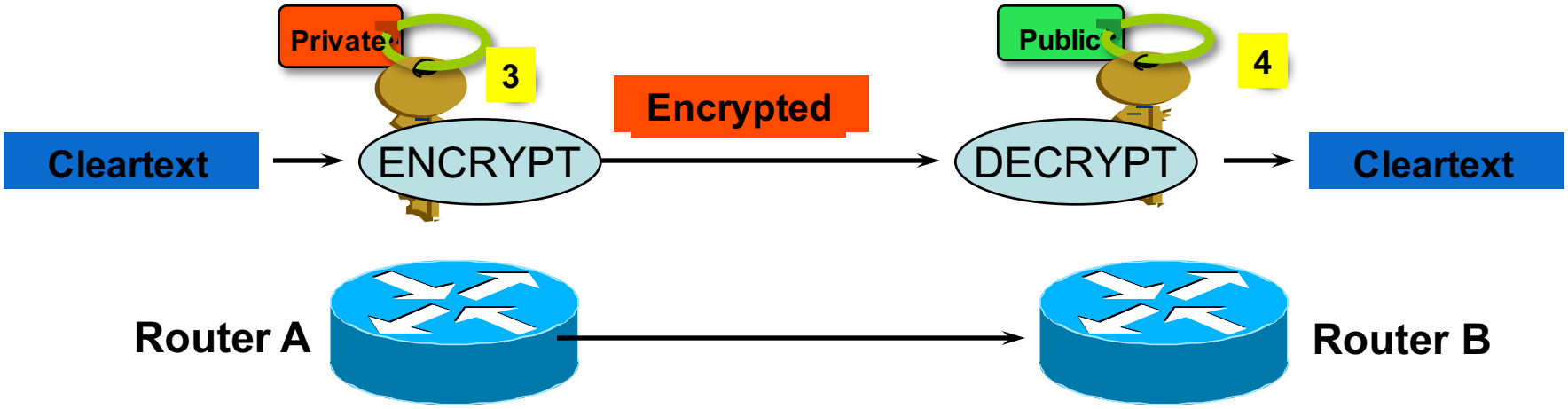
Authentication and Integrity (1)



1. Router A generates public/private key pair

2. Router A sends its public key to Router B

Authentication and Integrity (2)

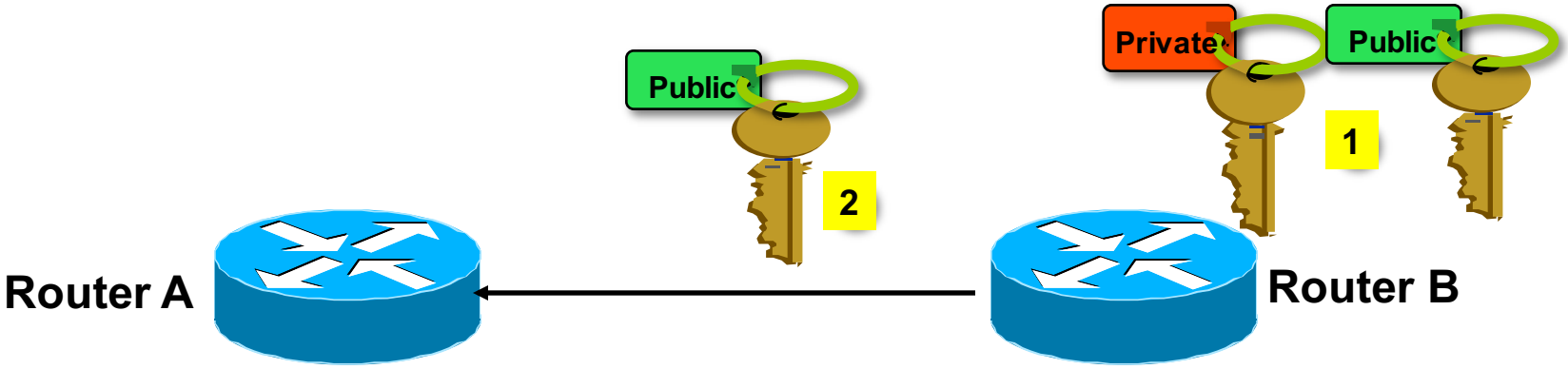


3. Router A encrypts packet with its private key and sends encrypted packet to Router B

4. Router B receives encrypted packet and decrypts with Router A's public key

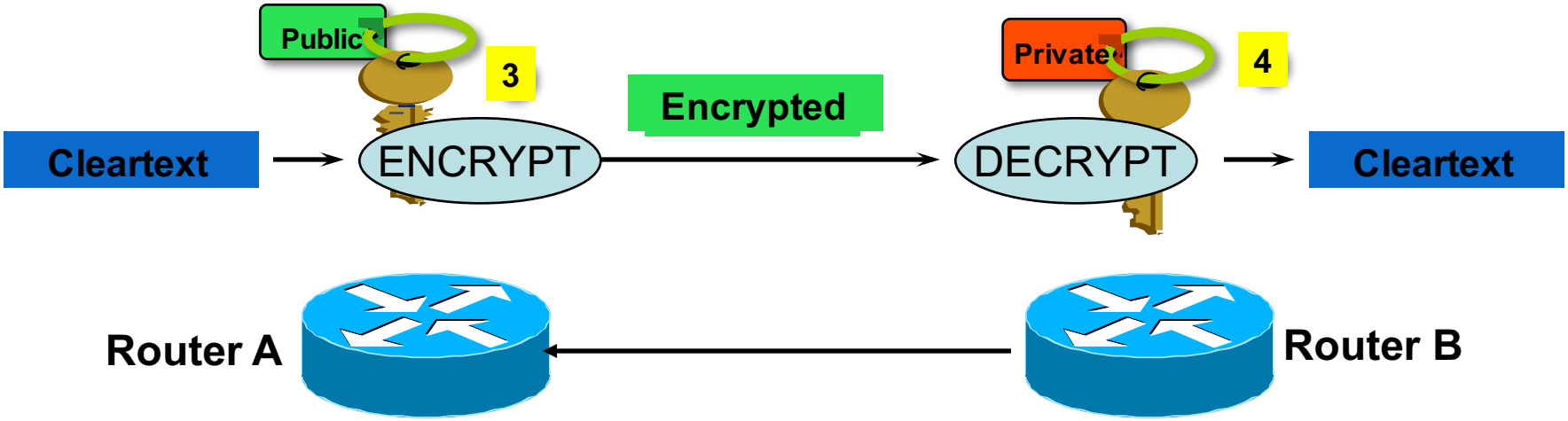
Since only Router A has its private key, you are reasonably Certain the data came from Router A

Data Confidentiality (1)



1. Router B generates public/private key pair
2. Router B sends its public key to Router A

Data Confidentiality (2)



3. Router A encrypts packet with router B's public key & sends encrypted packet to Router B
4. Router B receives encrypted packet and decrypts with its' private key

Since only Router B has its private key, it should be only one to decrypt the traffic

Cryptographic Keys

- Every principal has to have at least one key
- *Do not* reuse the same key for many conversations
  - Encrypting too much traffic in one key aids cryptanalysis—this has been known for more than 150 years
- Instead, must create a new key each time
- This process—*key setup*—is typically done by a *cryptographic protocol* such as SSL

Digital Signatures

- A digital signature is a message appended to a packet
- Used to prove the identity of the sender and the integrity of the packet

Digital Signatures

- Two common public-key digital signature techniques:
  - RSA (Rivest, Shamir, Adelman)
  - DSS (Digital Signature Standard)
- A sender uses its private key to sign a packet.
- The receiver of the packet uses the sender's public key to verify the signature.
- Successful verification assures:
  - The packet has not been altered
  - The identity of the sender

Public Key Infrastructure

- Mechanism to manage digital certificates
  - Whose public key?
  - What is the key good for?
- Supports scalable security services using public key cryptography
  - Authentication
  - Confidentiality
  - Data Integrity
  - Non-Repudiation

PKI Components

- Certification Authority
  - A trusted authority which issues digital certificates
  - Also publishes CRL (Certificate Revocation List)
- Registration Authority
  - An entity that is trusted by the CA to vouch for the identity of users to a CA
    - This entity is only trusted by the CA
    - Generally relies on operational controls and cryptographic security rather than physical security
- Repository
  - An electronic site that holds certificates and certificate status information
    - Need not be a trusted system since all information is tamper-evident
    - Most commonly accesses via LDAP
    - Theoretically could be accesses using HTTP, FTP or even electronic mail

Thank You