

# Transport Layer Security (TLS)

Assignment Project Exam Help

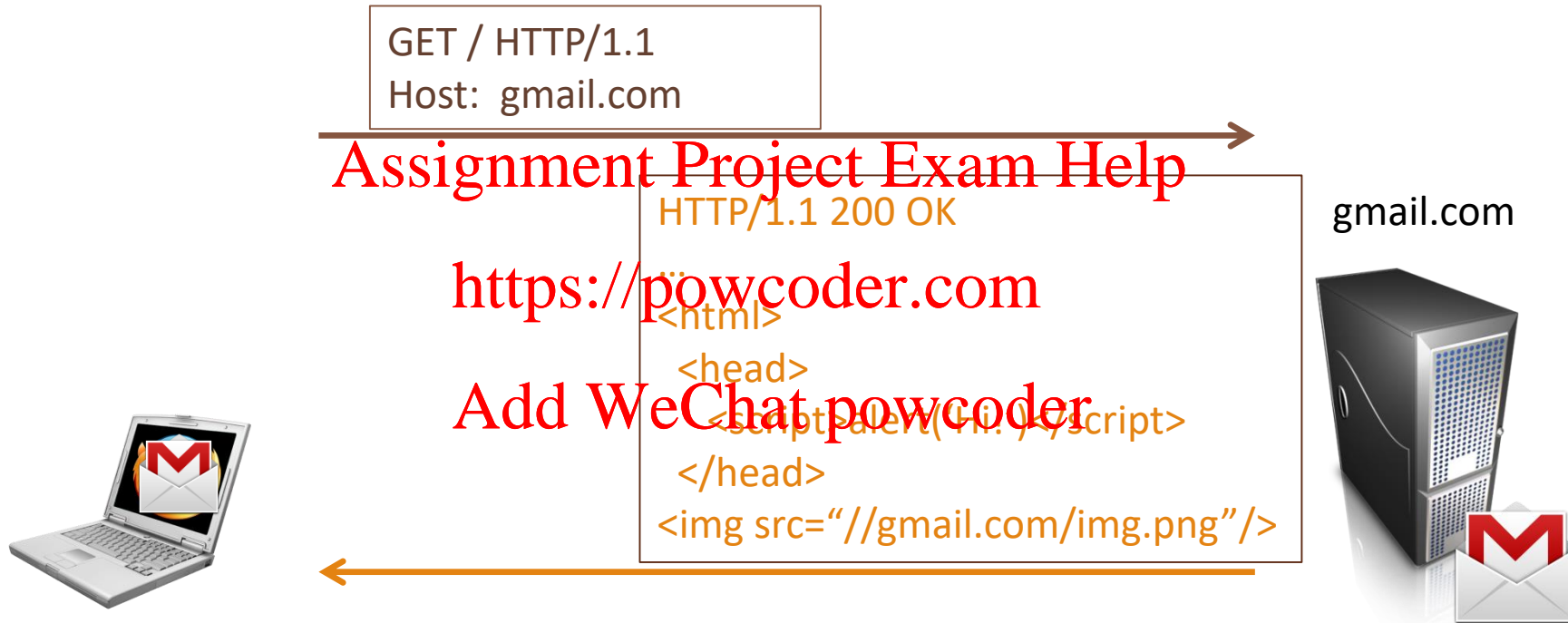
<https://powcoder.com>

Add WeChat powcoder

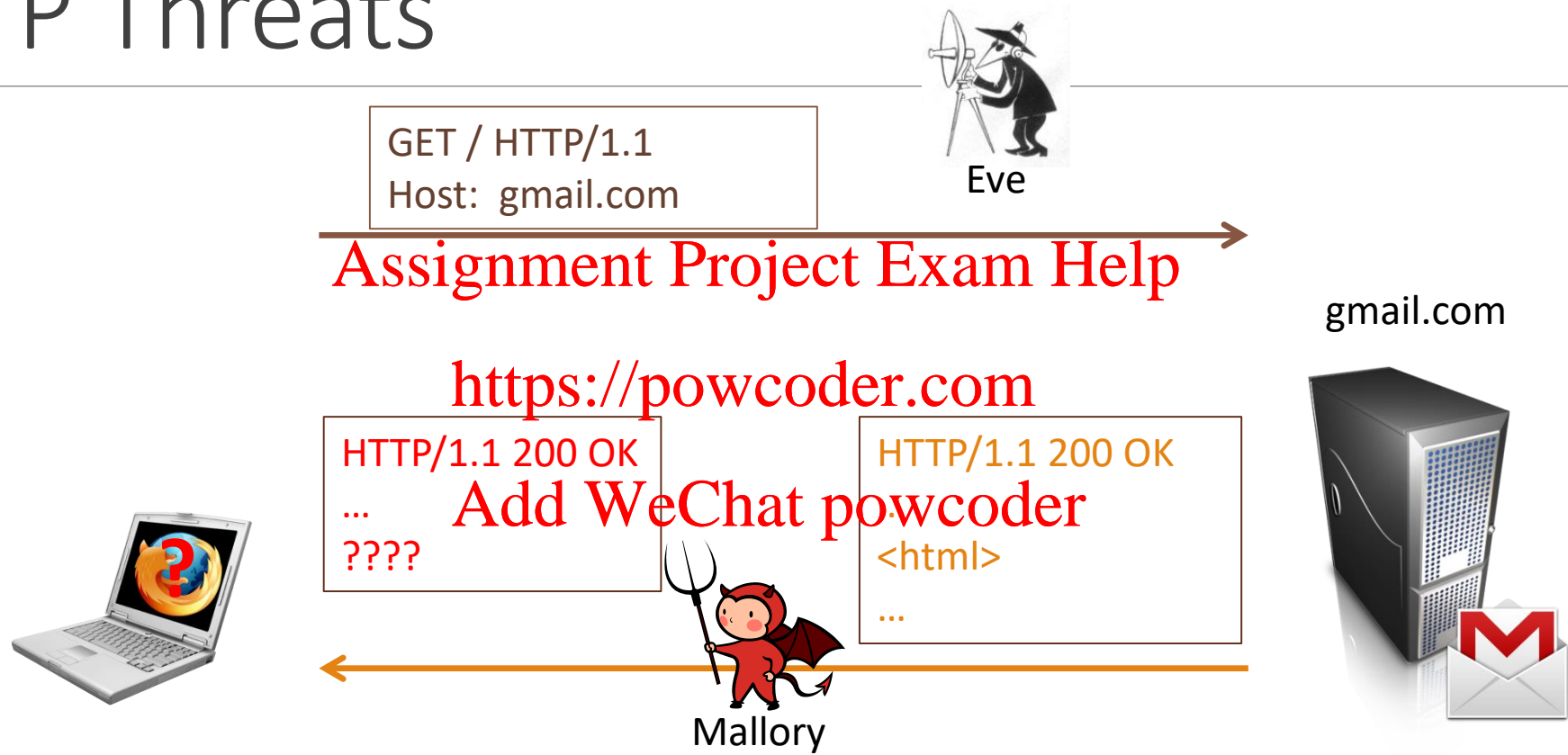
---

ECEN 4133  
Feb 18, 2021

# Review: HTTP



# HTTP Threats



# HTTP Threats

---

Eve can observe:

- What page you are visiting (e.g. <http://gmail.com/email84534>)
- Server response (e.g. the content of your email)
- Cookies (Can now login as you!)
- Submitted forms (passwords, new emails, credit cards, etc)

Mallory can:

- Provide you false information (e.g. change the content of an email)
- Change what data you send (e.g. change the contents of what you post/send!)
- Insert Javascript on your page (e.g. tracking info / steal information from gmail's origin)

Solution:

- Cryptography! Confidentiality + Integrity
  - ...but how?

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# How do we translate?

---

## Cryptographic Primitives

Symmetric  
Encryption

RSA

PKI

Certificate

HMAC

Public Key

RC4

Diffie-Hellman

DSA

ECDSA

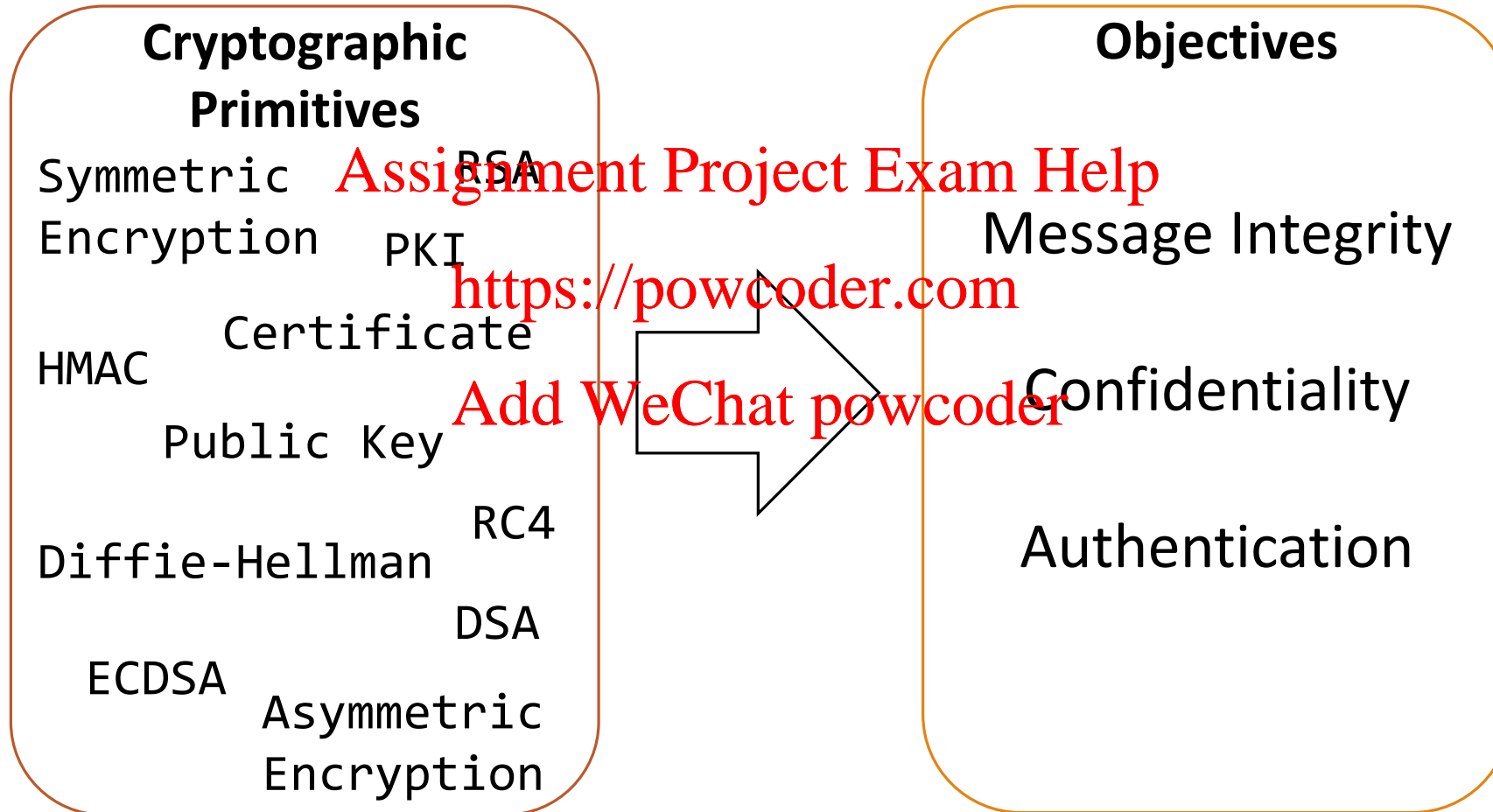
Asymmetric  
Encryption

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# How do we translate?



# How do we translate?

---

## Cryptographic Primitives

Symmetric  
Encryption

RSA

PKI

Certificate

HMAC

Public Key

RC4

Diffie-Hellman

DSA

ECDSA

Asymmetric  
Encryption

## Typical HTTPS Connection

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# HTTPS, TLS

---

## Transport Layer Security (TLS)

- Previous versions: Secure Socket Layer (SSL) – do not use!
  - SSL 2
  - SSL 3.0
- TLS 1.0, 1.1, 1.2 – extensions/improvements to SSL 3.0
- TLS 1.3 – redesigned TLS (2018)

HTTPS – the S stands for Secure

- HTTP over TLS

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



# Case Study: TLS

---

Arguably the most important (and widely used) cryptographic protocol on the Internet

**Assignment Project Exam Help**

Almost all encrypted protocols (minus SSH) uses TLS for transport encryption

**<https://powcoder.com>**

HTTPS, POP3, IMAP, SMTP, FTP, NNTP, XMPP (Jabber), OpenVPN, SIP (VoIP), ...

**Add WeChat powcoder**

# Browser TLS Support

Browser	Version	Platforms	SSL protocols		TLS protocols			
			SSL 2.0 (insecure)	SSL 3.0 (insecure)	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3 (proposed)
Google Chrome (Chrome for Android) [n 8] [n 9]	1–9	Windows (7+) OS X (10.9+) Linux Android (4.1+) iOS (9.0+) Chrome OS	Disabled by default	Enabled by default	Yes	No	No	No
	10–20		No <sup>[48]</sup>	Enabled by default	Yes	No	No	No
	21		No	Enabled by default	Yes	No	No	No
	22–25		No	Enabled by default	Yes	Yes <sup>[50]</sup>	No <sup>[50][51][52][53]</sup>	No
	26–29		No	Enabled by default	Yes	Yes	No	No
	30–32		No	Enabled by default	Yes	Yes	Yes <sup>[51][52][53]</sup>	No
	33–37		No	Enabled by default	Yes	Yes	Yes	No
	38, 39		No	Enabled by default	Yes	Yes	Yes	No
	40		No	Disabled by default <sup>[55][59]</sup>	Yes	Yes	Yes	No
	41, 42		No	Disabled by default	Yes	Yes	Yes	No
	43		No	Disabled by default	Yes	Yes	Yes	No

# Browser TLS support

Google Chrome (Chrome for Android) [n 8] [n 9]	41, 42	Windows (7+) macOS (10.11+) Linux Android (5.0+) iOS (12.2+) Chrome OS	No	Disabled by default	Yes	Yes	Yes	No
	43		No	Disabled by default	Yes	Yes	Yes	No
	44–47		No	No <sup>[93]</sup>	Yes	Yes	Yes	No
	48, 49		No	No	Yes	Yes	Yes	No
	50–53		No	No	Yes	Yes	Yes	No
	54–66		No	No	Yes	Yes	Yes	Disabled by default (draft version)
	67–69		No	No	Yes	Yes	Yes	Yes (draft version)
	70–83		No	No	Yes	Yes	Yes	Yes
	84–87	88	No	No	Warn by default	Warn by default	Yes	Yes
	91 <sup>[97]</sup>		No	No	No	No	Yes	Yes
Browser	Version	Platforms	SSL 2.0 (insecure)	SSL 3.0 (insecure)	TLS 1.0 (deprecated)	TLS 1.1 (deprecated)	TLS 1.2	TLS 1.3

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Where does TLS live?

---

Application (HTTP)

Transport (TCP)

Network (IP)

Data-Link (1gigE)

Physical (copper)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



Client

Server

“the handshake”

Assignment Project Exam Help

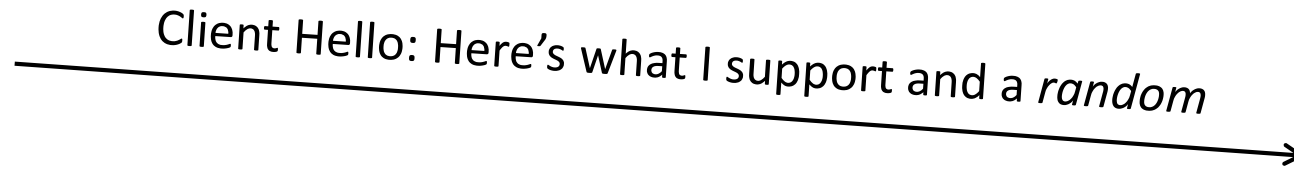
<https://powcoder.com>

Add WeChat powcoder

Client

Server

Client Hello: Here's what I support and a *random*



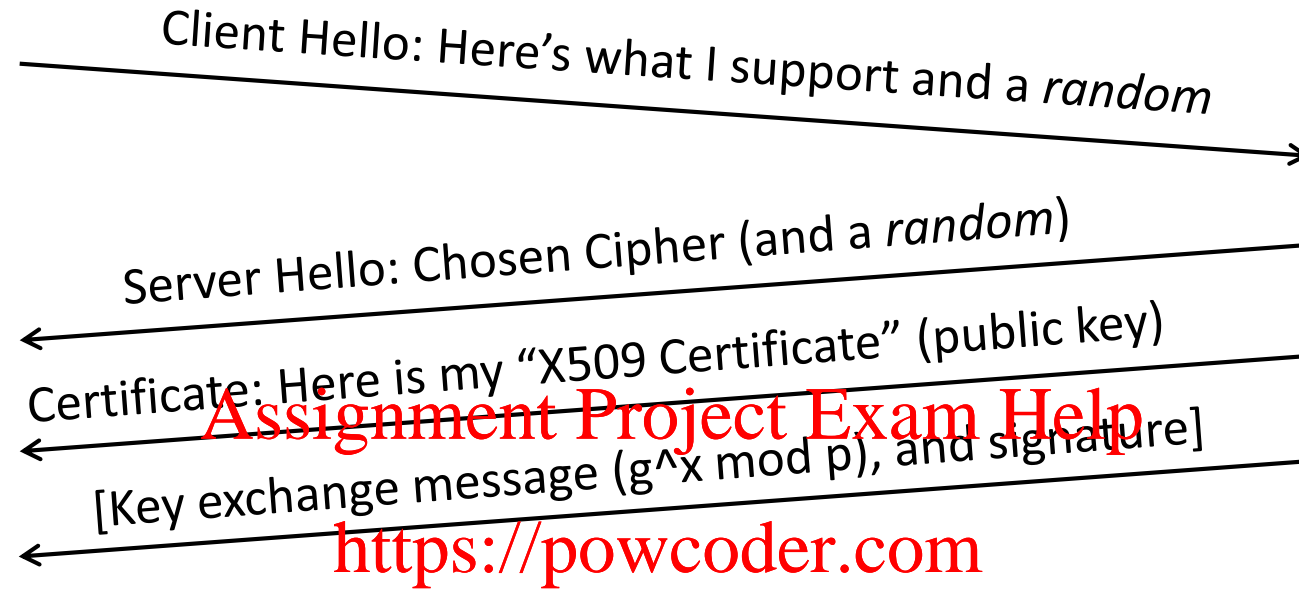
Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Client

Server



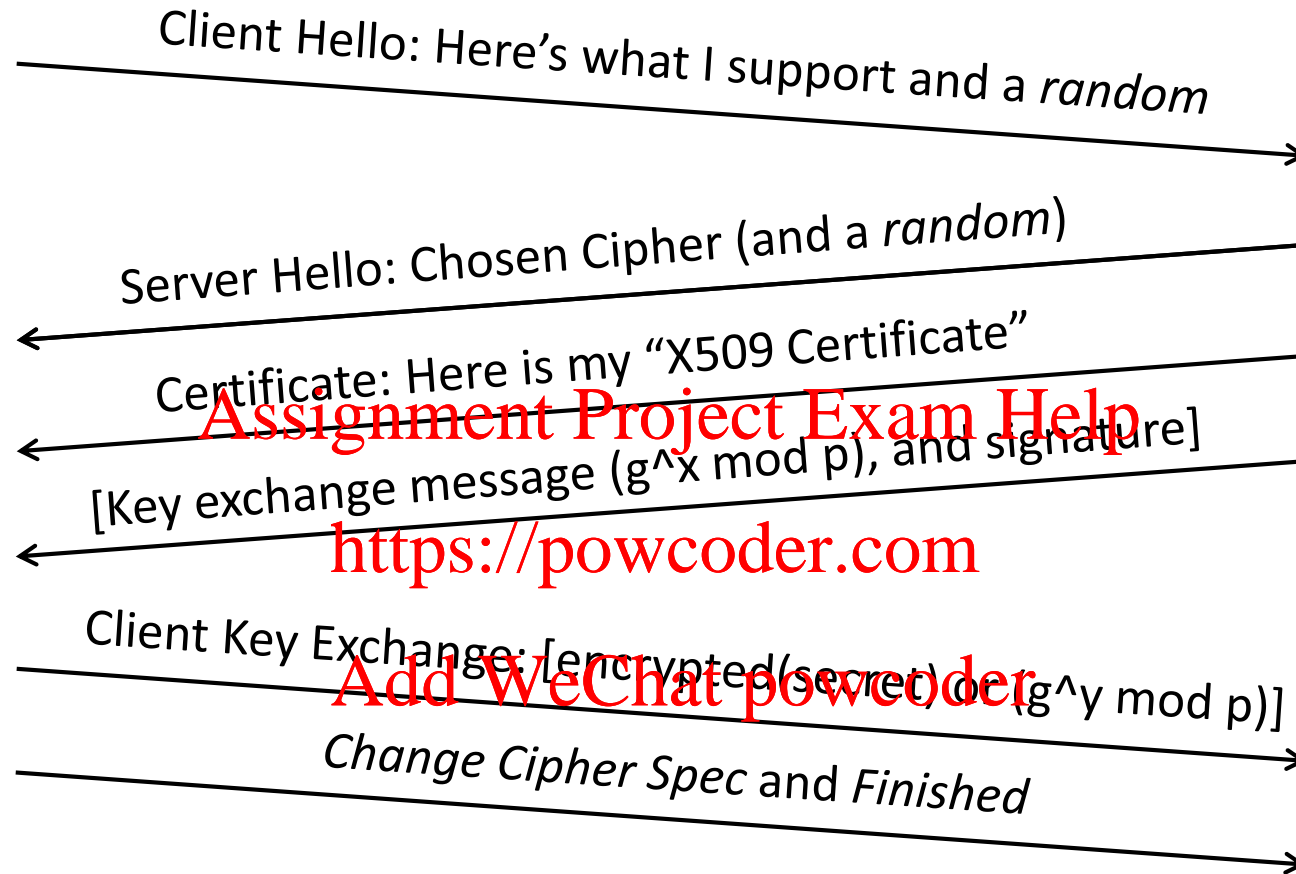
Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Client

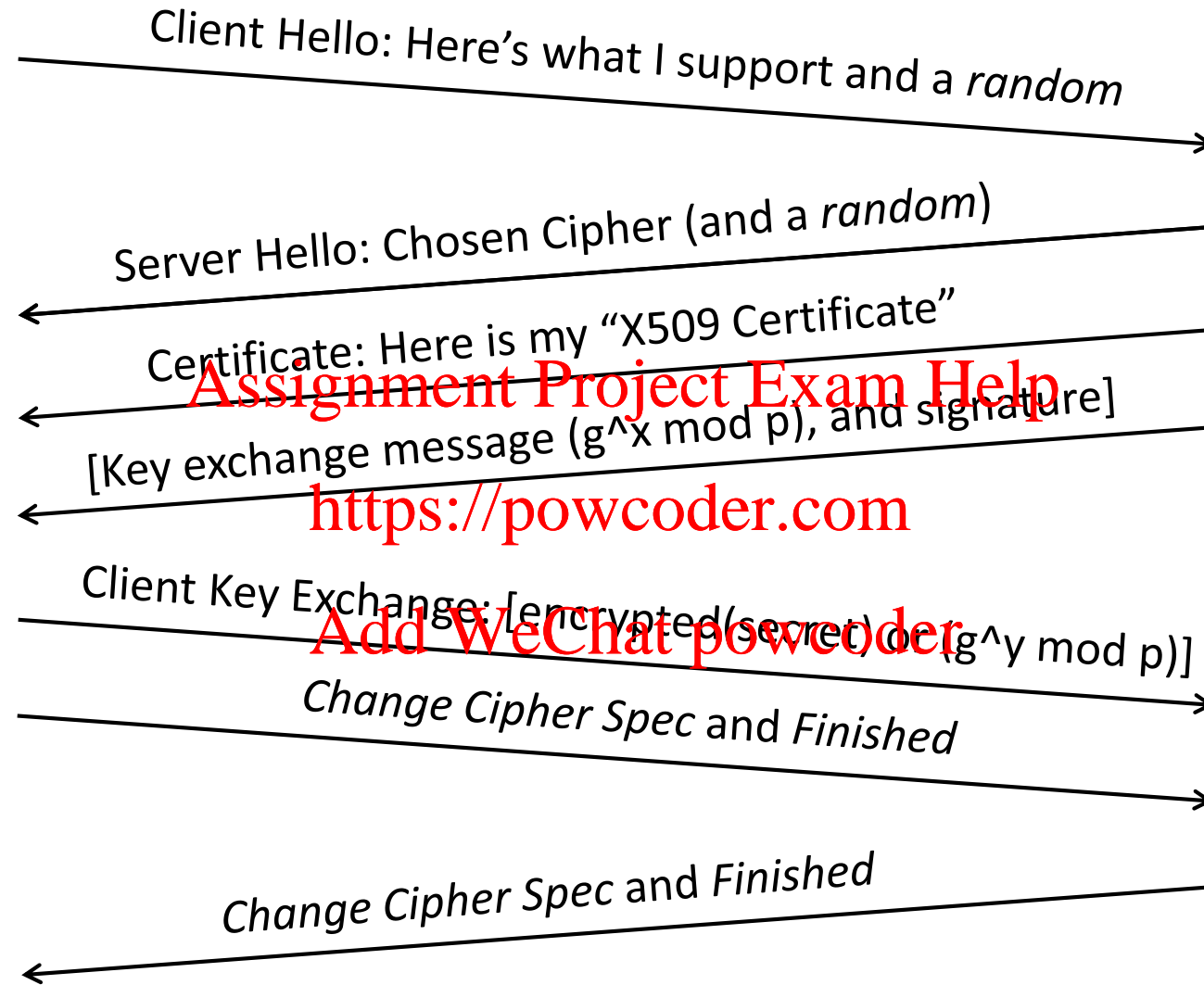
Server





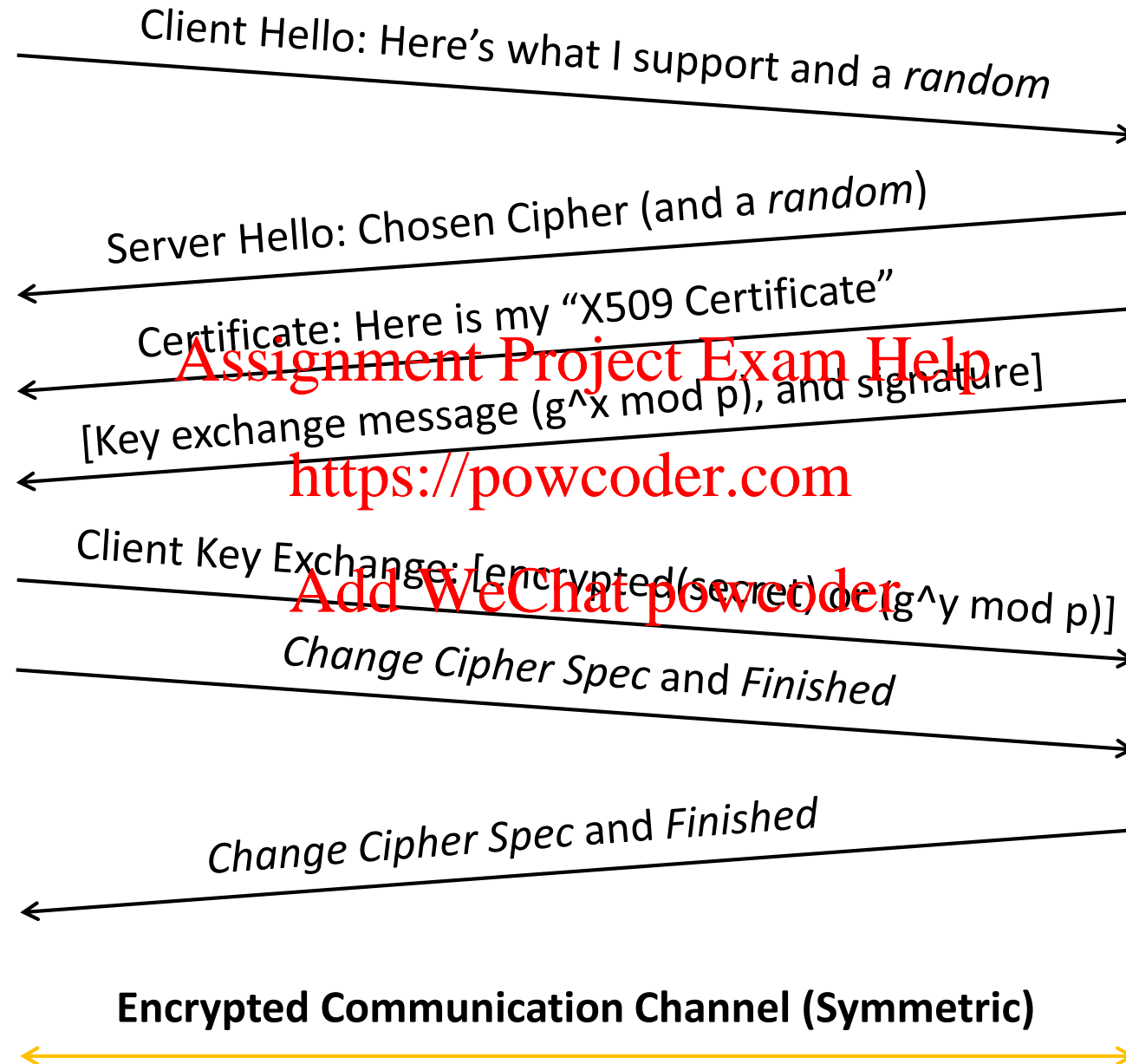
Client

Server



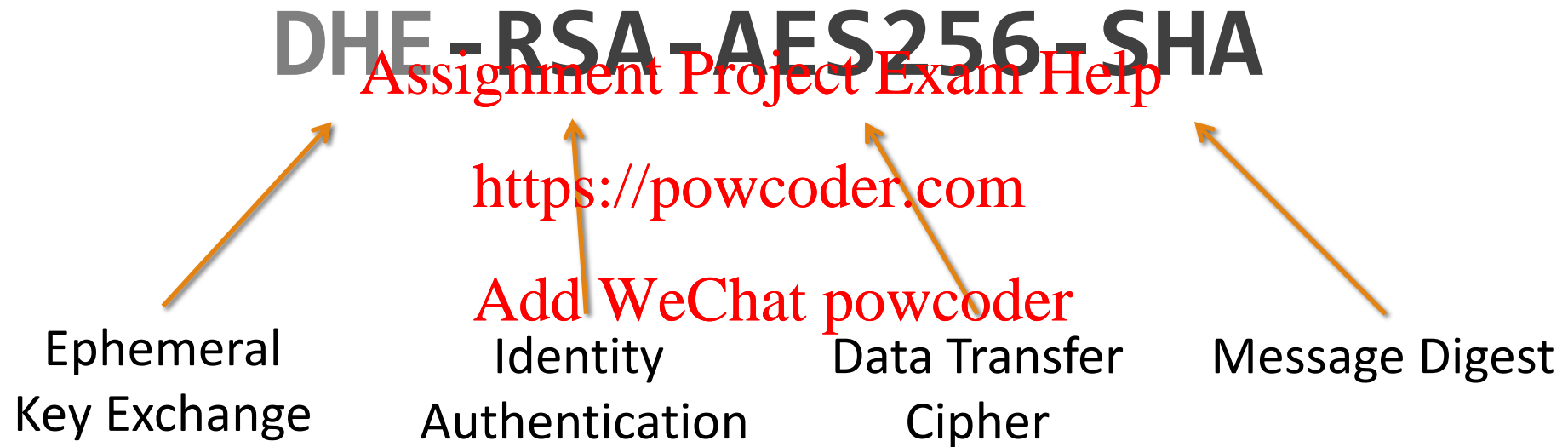
Client

Server



# Cipher Suites

---



🔍 📄 | Console Elements Sources Network Timeline Profiles Application Security Audits Adblock Plus

🔒 Overview

Main Origin

● <https://www.google.com>

Secure Origins

● <https://ssl.gstatic.com>

● <https://lh3.googleusercontent.com>

● <https://www.gstatic.com>

● <https://clients5.google.com>

● <https://apis.google.com>

● <https://plus.google.com>

● <https://www.google.com>  
[View requests in Network Panel](#)

Connection

Protocol **QUIC**

Key Exchange **ECDHE\_RSA**

Cipher Suite **AES\_128\_GCM**

Certificate

Subject **.google.com**

SAN **\*.google.com**

**\*.android.com**  
[Show more \(53 total\)](#)

Valid From **Wed, 14 Sep 2016 08:26:35 GMT**

Valid Until **Wed, 07 Dec 2016 08:19:00 GMT**

Issuer **Google Internet Authority G2**

SCTs **2 valid SCTs**

[Open full certificate details](#)

The security details above are from the first inspected response.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Goals

---



Confidentiality

Assignment Project Exam Help



<https://powcoder.com>  
Message Integrity

Add WeChat powcoder



Authentication

# X509 Certificates

**Subject:** C=US/O=Google Inc/CN=www.google.com

**Issuer:** C=US/O=Google Inc/CN=Google Internet Authority

**Serial Number:** 01:b1:04:17:be:22:48:b4:8e:1e:8b:a0:73:c9:ac:83

**Expiration Period:** Jul 12 2010 - Jul 19 2012

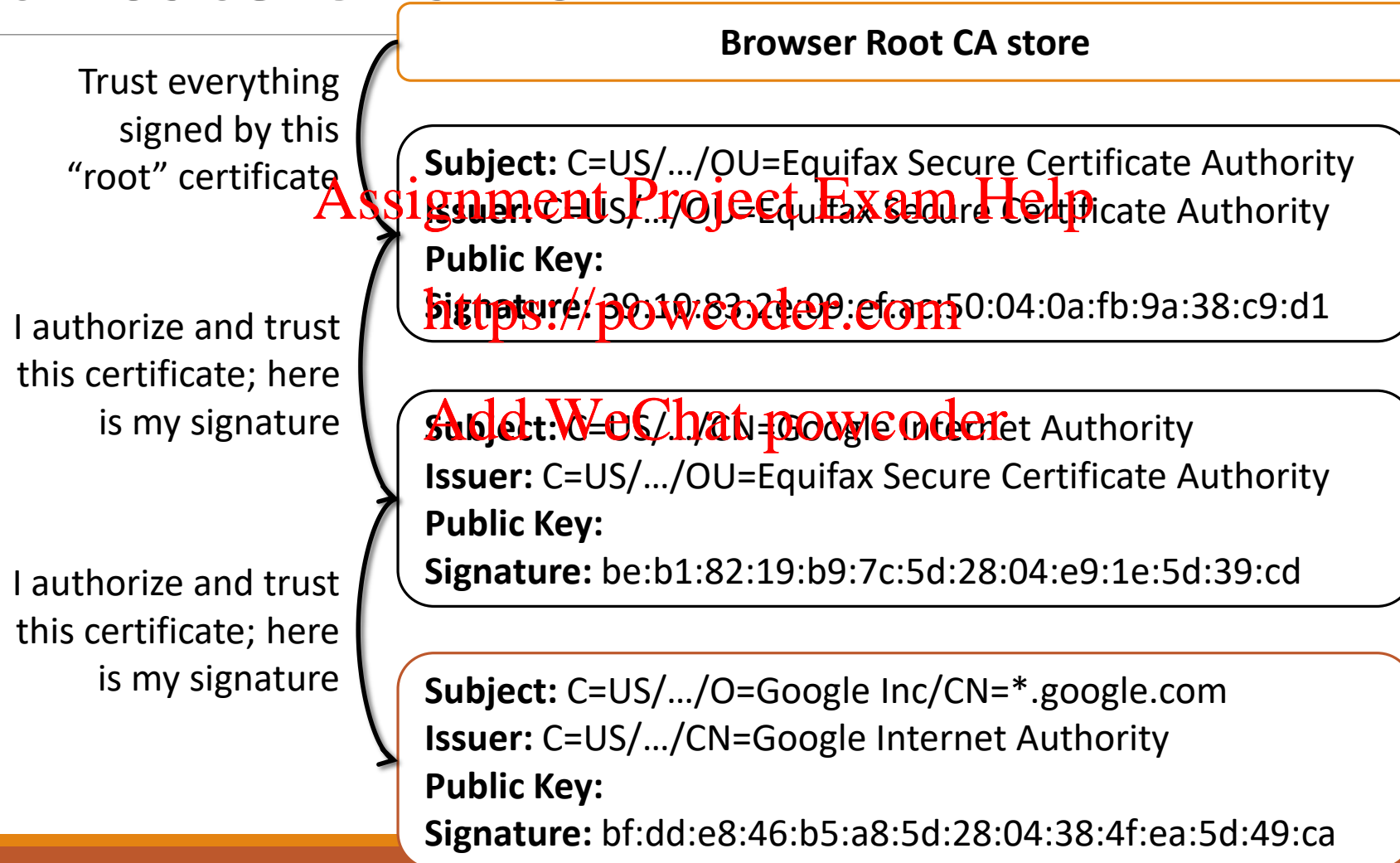
**Public Key Algorithm:** rsaEncryption

**Public Key:** 43:1d:53:2e:09:ef:dc:50:54:0a:fb:9a:f0:fa:14:58:ad:a0:81:b0:3d  
7c:be:b1:82:19:b9:7c3:8:04:e9:1e5d:b5:80:af:d4:a0:81:b0:b0:68:5b:a4:a4  
:ff:b5:8a:3a:a2:29:e2:6c:7c3:8:04:e9:1e5d:b5:7c3:8:04:e9:39:23:46

**Signature Algorithm:** sha1WithRSAEncryption

**Signature:** 39:10:83:2e:09:ef:ac:50:04:0a:fb:9a:f0:fa:14:58:ad:a0:81:b0:3d  
7c:be:b1:82:19:b9:7c3:8:04:e9:1e5d:b5:80:af:d4:a0:81:b0:b0:68:5b:a4:a4  
:ff:b5:8a:3a:a2:29:e2:6c:7c3:8:04:e9:1e5d:b5:7c3:8:04:e9:1e5d:b5

# Certificate Chains



# Goals

---



Confidentiality (Symmetric Crypto)

Assignment Project Exam Help



<https://powcoder.com>  
Message Integrity (HMACs)

Add WeChat powcoder



Authentication (Public Key Crypto)



# Certificate Authority Ecosystem

---

Each browser trusts a set of CAs

CAs can sign certificates for new CAs

CAs can sign certificates for any website

Assignment Project Exam Help

<https://powcoder.com>

If a single CA is compromised, then the entire system is compromised

Add WeChat powcoder

We ultimately place our complete trust of the Internet in the weakest CA

# Immediate Concerns

---

Nobody has any idea who these CAs are...

1,500+ known browser trusted CAs

Assignment Project Exam Help

<https://powcoder.com>

History of CAs being hacked (e.g. Diginotar)

Add WeChat powcoder

Oooops, Korea gave every elementary school, library, and agency a CA certificate (1,324)

- Luckily invalid due to a higher-up constraint

# Getting a Certificate

---

Certificates are free and easy to get!

<https://letsencrypt.org/>  
Assignment Project Exam Help

<https://powcoder.com>

Identity validated via e-mail in whois, or proving control over a certain webpage on the domain

- What can go wrong?

Add WeChat powcoder

Setting up TLS manually is hard. People are terrible at it!

# DigiNotar

---

DigiNotar ***was*** a Dutch Certificate Authority

On June 10, 2011, \*.**google.com** cert was issued to an attacker and subsequently used to orchestrate MITM attacks in Iran

<https://powcoder.com>

Nobody noticed the attack until someone found the certificate in the wild... and posted to *pastebin*

[Add WeChat powcoder](#)

# DigiNotar Contd.

---

DigiNotar later admitted that dozens of fraudulent certificates were created

Google, Microsoft, Apple and Mozilla all revoked the root Diginotar certificate

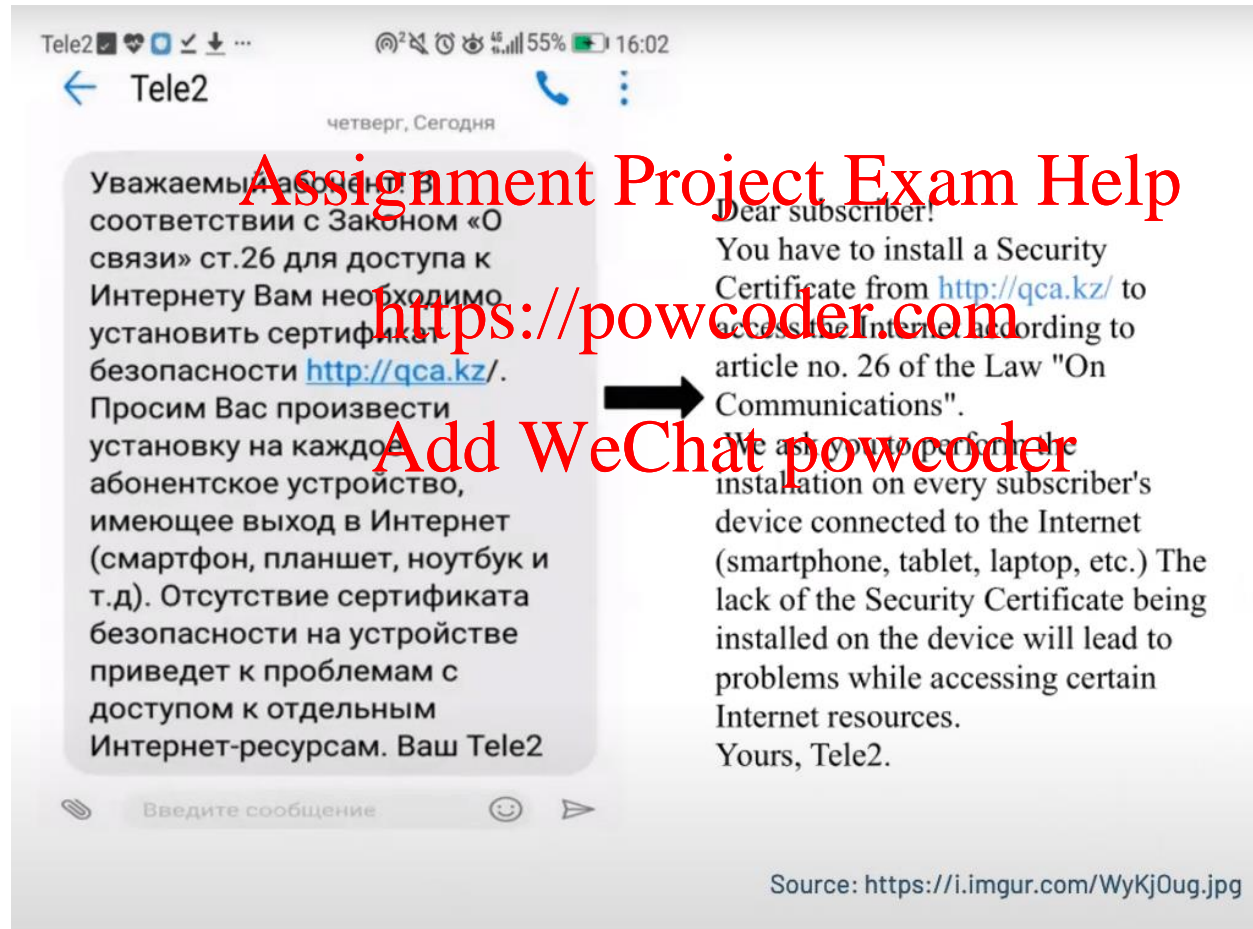
<https://powcoder.com>

Dutch Government took over Diginotar

Add WeChat powcoder

Diginotar went bankrupt and died

# Kazakhstan TLS MITM



# Kazakhstan TLS MITM

[illegible]

# Kazakhstan TLS MITM

---

Domains impacted:

allo.google.com, android.com, cdninstagram.com, dns.google.com, docs.google.com, encrypted.google.com, facebook.com, geo.g, google.com, groups.google.com, hangouts.google.com, instagram.com, mail.google.com, mail.ru, messages.android.com, messenger.com, news.google.com, pl.ru, picasa.google.com, plus.google.com, rukueb.com, sites.google.com, sosalkino.tv, tamtam.chat, translate.google.com, twitter.com, video.google.com, vk.com, vk.me, vkuseraudio.net, vkuservideo.net, www.facebook.com, www.google.com, www.instagram.com, www.messenger.com, www.youtube.com, youtube.com

Browser response:

- Remove KZ root cert *even if user explicitly added it!*



# Attack Vectors

---

Attack the weakest Certificate Authority

Attack browser implementations

Assignment Project Exam Help

<https://powcoder.com>

Magically notice a bug in a key generation library that leads you to discovering all the private keys on the Internet

Add WeChat powcoder

Attack the cryptographic primitives

- Math is hard, let's go shopping!

# TLS Attacks

---

## User concerns

- Deploying site leaks private key
- Client users ignore HTTPS errors!

Assignment Project Exam Help

## Attack (weakest) CA

- DigiNotar, Comodo, WoSign/Startcom

<https://powcoder.com>

## Attack Browser

- SSL Strip, Null Prefix, Padding Oracle, BEAST, CRIME, goto fail, POODLE, FREAK, LogJam, DROWN, ...

Add WeChat powcoder

## Attack Server

- Heartbleed



"-----BEGIN RSA PRIVATE KEY-----" -openssl



Search

About 274,000 results (0.24 seconds)

G

Everything

Images

Maps

Videos

News

Shopping

More

All results

Related searches

More search tools

[-----BEGIN RSA PRIVATE KEY - Pastebin.com - #1 paste tool since ...](#)

[pastebin.com/TbaeU93m](#)

19 Apr 2010 – ... the difference. Copied. -----BEGIN RSA PRIVATE KEY-----.

MIICXwIBAAKBpenis1ePqHkVN9IKaGBESjV6zBrIsZc+XQYTtSIVa9R/4SAXoYpl ...

[-----BEGIN RSA PRIVATE KEY - Pastebin.com - #1 paste tool since ...](#)

[pastebin.com/sC7bGw30](#)

18 Apr 2010 – ... difference. Copied. -----BEGIN RSA PRIVATE KEY-----.

MIIEogIBAAKCAQEA1BshzKMeyLmV7ptL1g7F5FWGFYj20AHLqm3+0+gpPbk ...

[site:pastebin.com "-----BEGIN RSA PRIVATE KEY-----" - Posterous](#)

[cdevers.posterous.com/repastebin.com/-----begin-rsa-private-key-----](#)

20 Apr 2010 – Apr 19, 2010 ... -----BEGIN RSA PRIVATE KEY-----

MIICXwIBAAKBpenis1ePqHkVN9IKaGBESjV6zBrIsZc+ XQYTtSIVa9R/4SAXoYpl .

[help/en/howto/sftp – Cyberduck](#)

[trac.cyberduck.ch/wiki/help/en/howto/sftp](#)

Private keys containing a DSA or RSA private key in PEM format are supported (look for -----BEGIN DSA PRIVATE KEY----- or -----BEGIN RSA PRIVATE KEY----- ...

[SSH access with a private RSA key \[Archive\] - VanDyke Software For...](#)

[forums.vandyke.com/archive/index.php/t-2185.html](#)

2 Sep 2011 – -----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQBujdbtxyIX4KaQPdTf5F/  
aOSBwSpZN4MjTixU2Yq8JkipjMYpYwpNj1TODzRjf ...

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# SSL Strip

Discovered by Moxie Marlinspike, 2009



GET / HTTP/1.1  
Host: bank.com

Assignment Project Exam Help

HTTP/1.1 301 Moved Permanently

Location: https://powcoder.com/  
https://powcoder.com

Add WeChat powcoder

[TLS Connection]

bank.com



# SSL Strip

Discovered by Moxie Marlinspike, 2009



# Null Termination Attack

Discovered by Moxie Marlinspike, 2009

---

ASN.1 utilizes Pascal-style strings

Web browsers utilize use C-style strings

Assignment Project Exam Help

<https://powcoder.com>  
gmail.com.evil.com

Add WeChat powcoder

gmail.com\0.evil.com

```
strcmp("gmail.com\0.evil.com", "gmail.com") == 0
```

# BEAST attack

Discovered by Thai Duong and Juliano Rizzo, 2011

---

“Browser Exploit Against SSL/TLS”

Chosen Plaintext attack against CBC-mode

Assignment Project Exam Help

Attacker can:

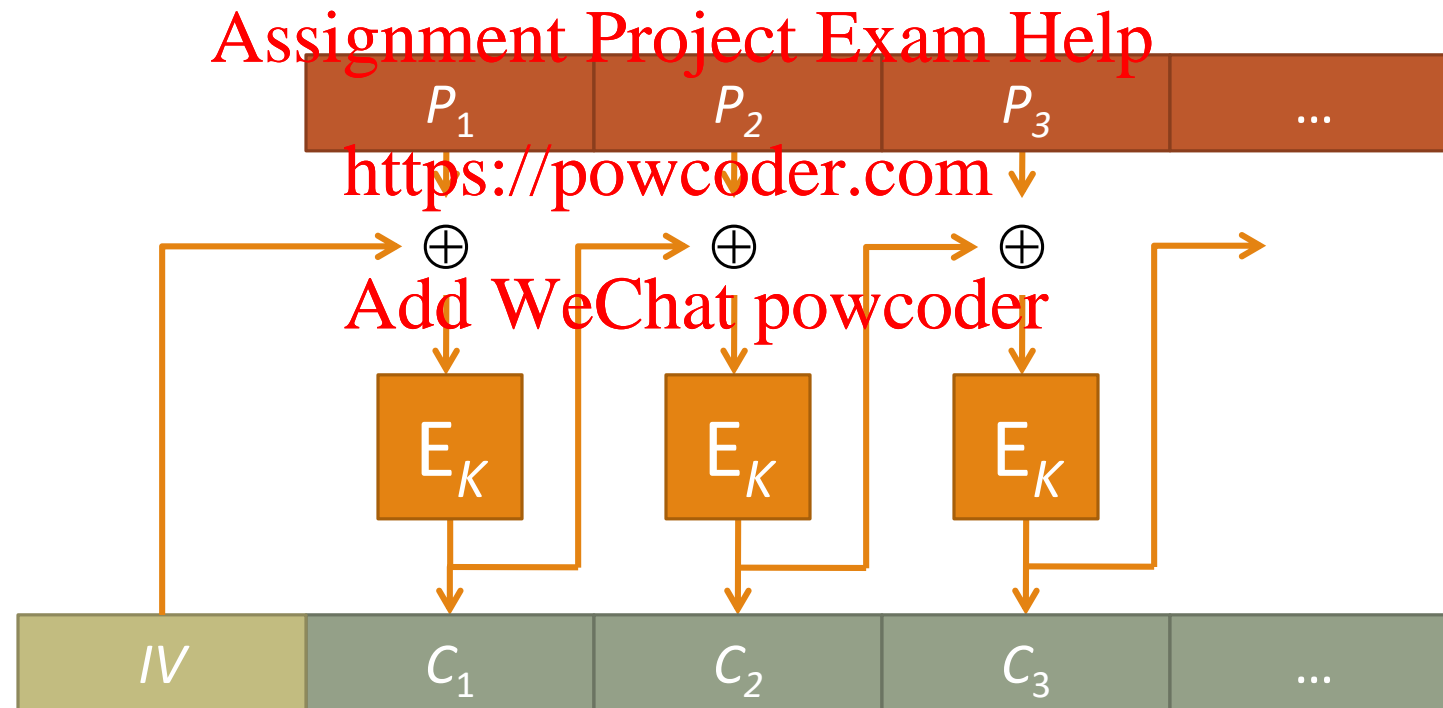
<https://powcoder.com>

- Observe Alice’s Ciphertext
- Make Alice to send **secret plaintext** P over TLS
  - E.g. HTTP Cookie
- Make Alice to send **arbitrary plaintext** over same TLS session

Add WeChat powcoder

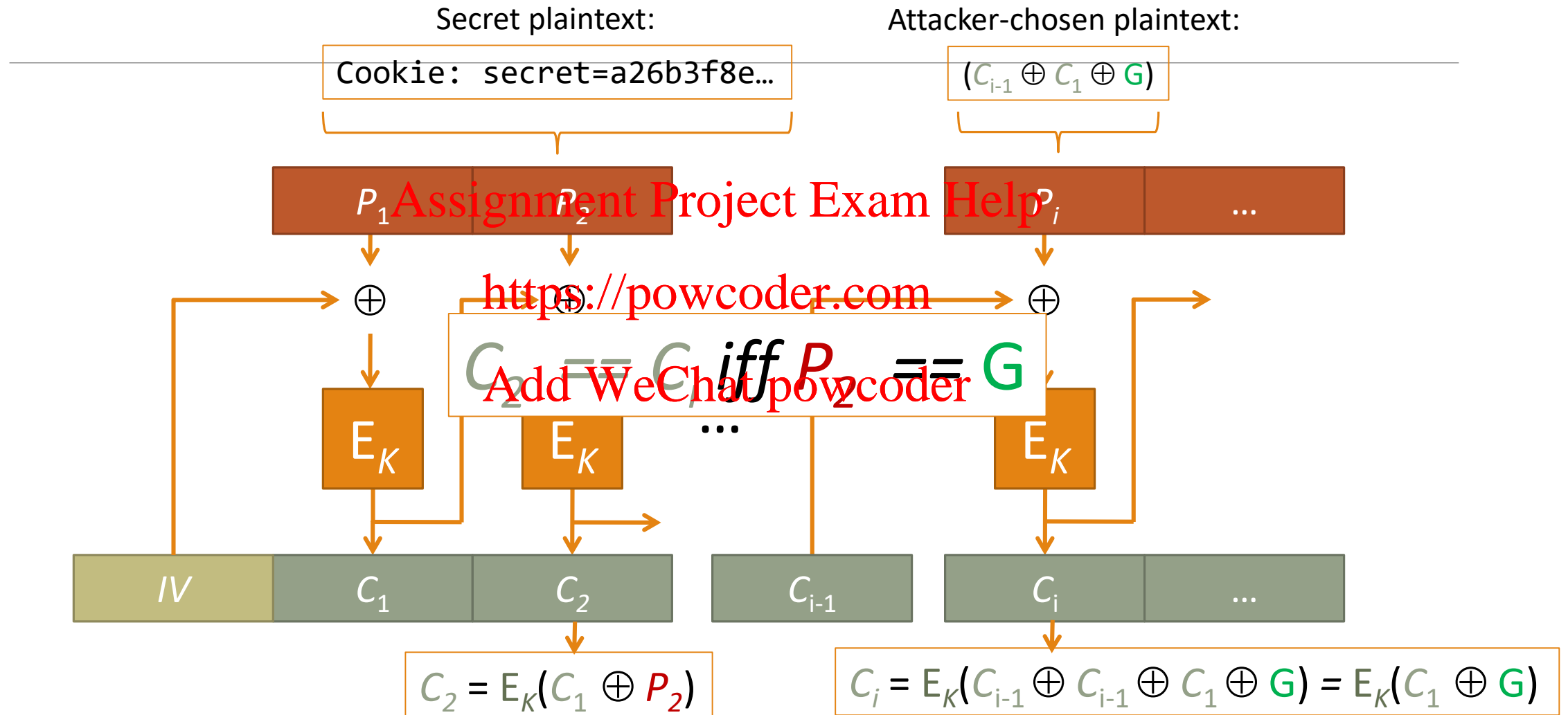
# CBC: Cipher-Block Chaining Mode

$$C_i := E(K, P_i \oplus C_{i-1}) \quad \text{for } i = 1, \dots, n$$





# BEAST attack



# BEAST attack

---

Problem: Attacker has to guess **G** entirely

Solution: force part of  $P_2$  to be known padding!

Cookie: secret=a26b3f8e...

$P_2$  ↓ Add WeChat powcoder  $P_3$

AAAAA\r\nCookie: secret=a 26b3f8e...

Only have to guess 1-byte now!

- 256 guesses and we're sure to get it

# BEAST attack

---

Once we guess a, we can redo the attack, with less padding:

Assignment Project Exam Help

$P_2$

$P_3$

AAAA\r\nCookie: secret=a2	6b3f8e...
---------------------------	-----------

Add WeChat powcoder

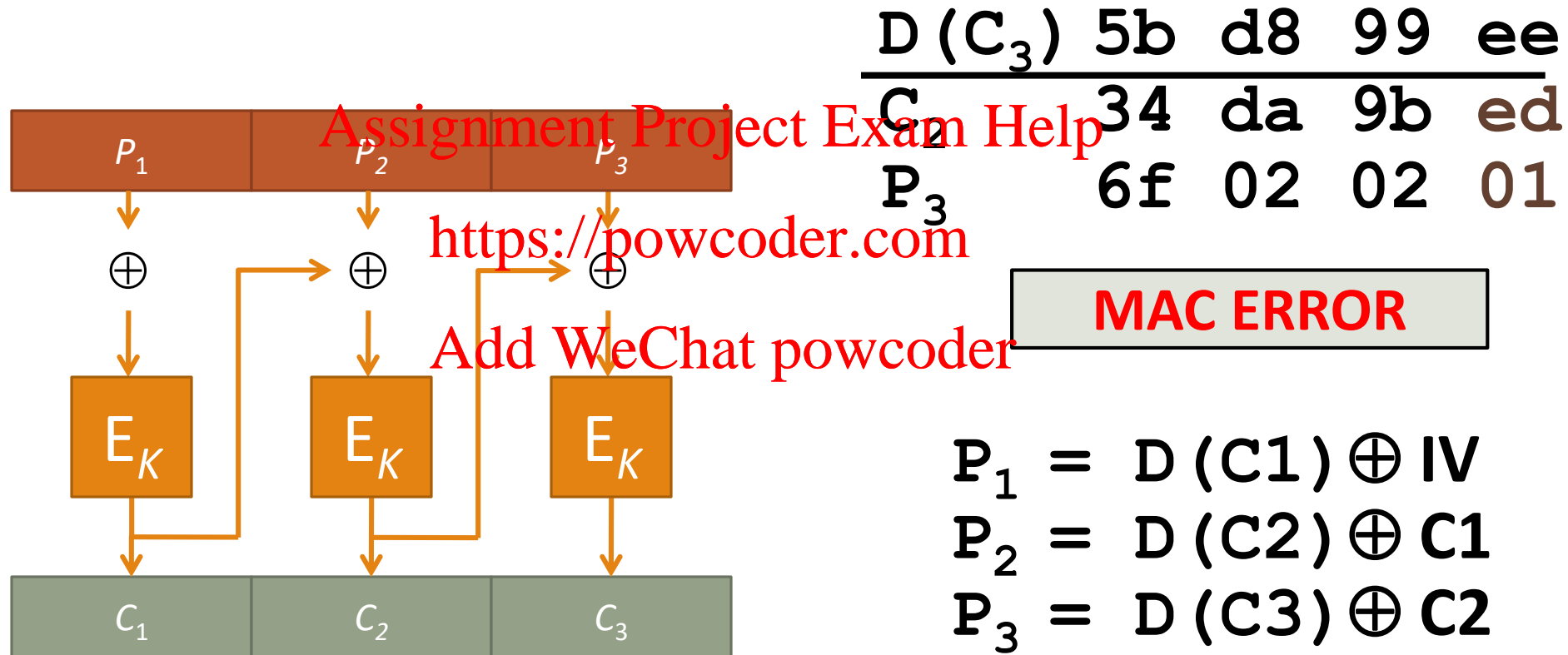
AAA\r\nCookie: secret=a26	b3f8e...
---------------------------	----------

AA\r\nCookie: secret=a26b	3f8e...
---------------------------	---------

A\r\nCookie: secret=a26b3	f8e...
---------------------------	--------

# Padding oracle attack

Discovered by Serge Vaudenay, 2003



# CRIME attack

Discovered by Thai Duong and Juliano Rizzo, 2012

---

## Compression Ratio Info-leak Made Easy

### Client compresses HTTP header

- Contains attacker controlled AND secret data!!

Assignment Project Exam Help

<https://powcoder.com>

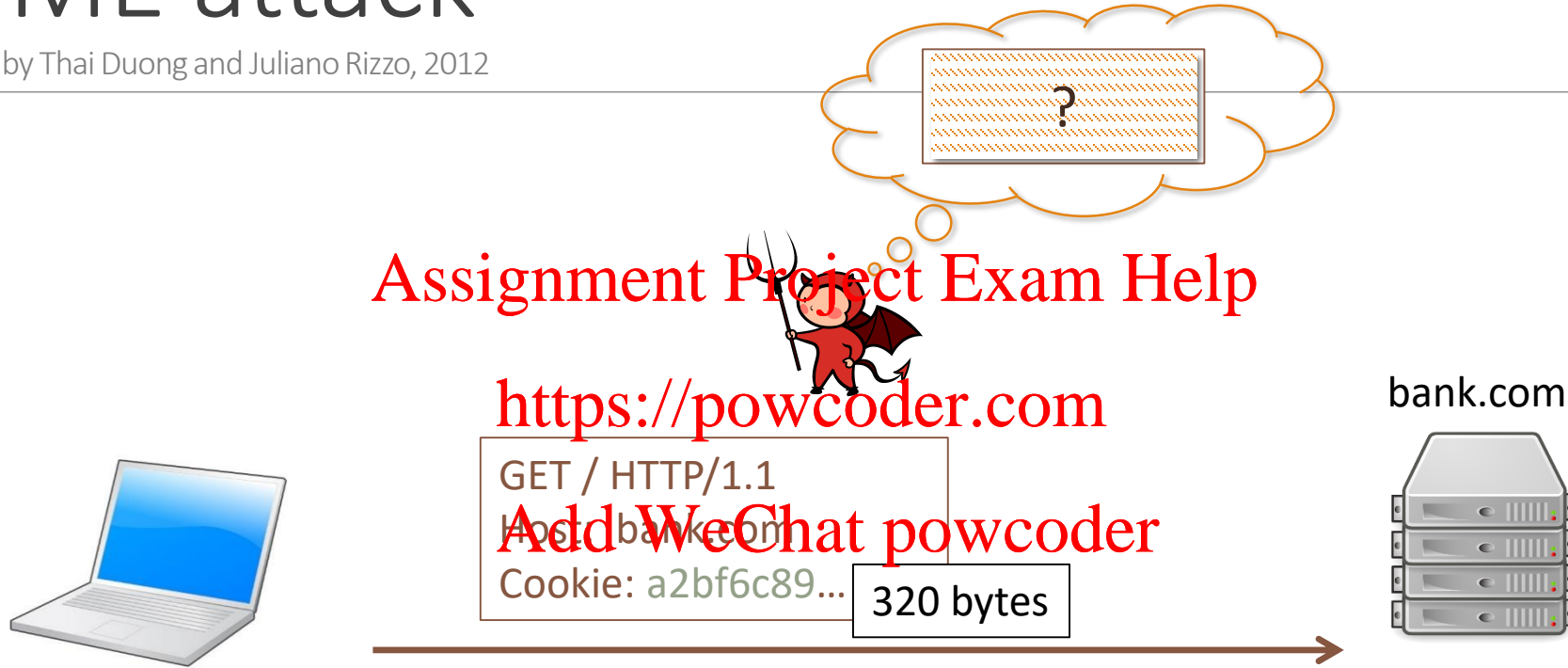
### Attacker can:

- Make Alice send HTTPS requests with some data controlled by the attacker, some data secret
- Observe encrypted data (length)

Add WeChat powcoder

# CRIME attack

Discovered by Thai Duong and Juliano Rizzo, 2012



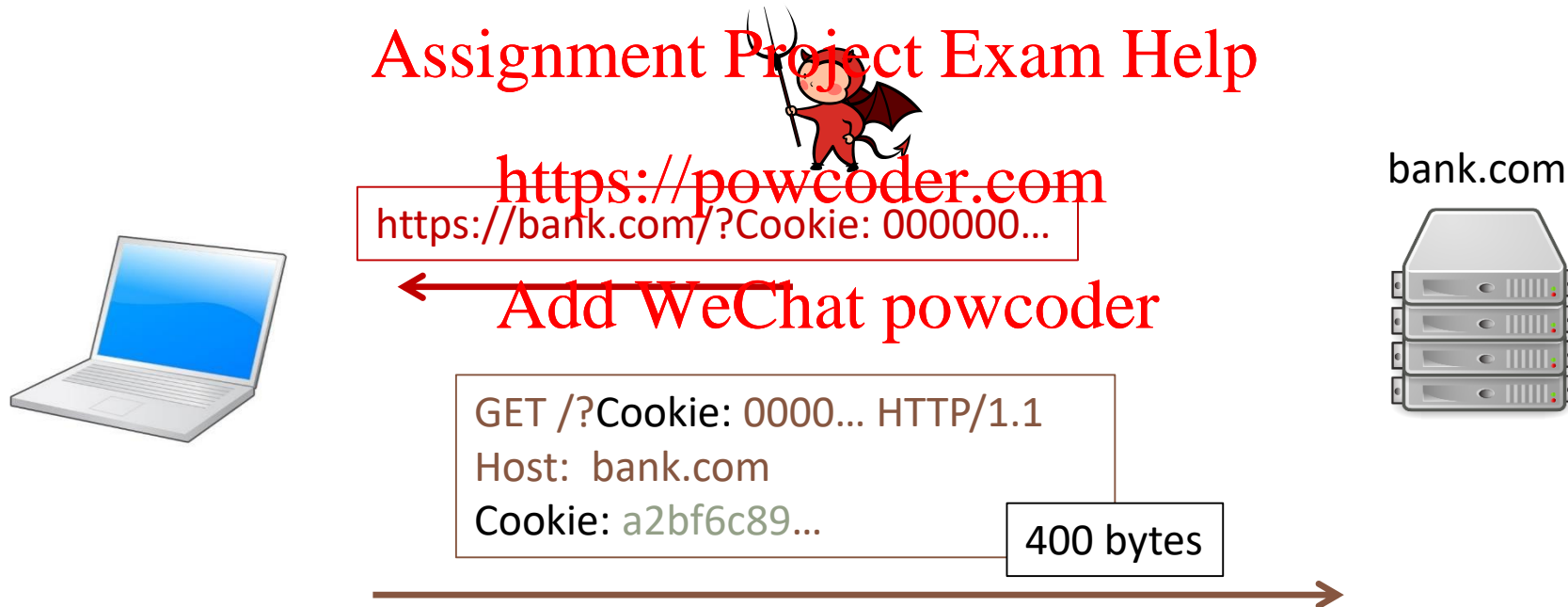
Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# CRIME attack

Discovered by Thai Duong and Juliano Rizzo, 2012



# CRIME attack

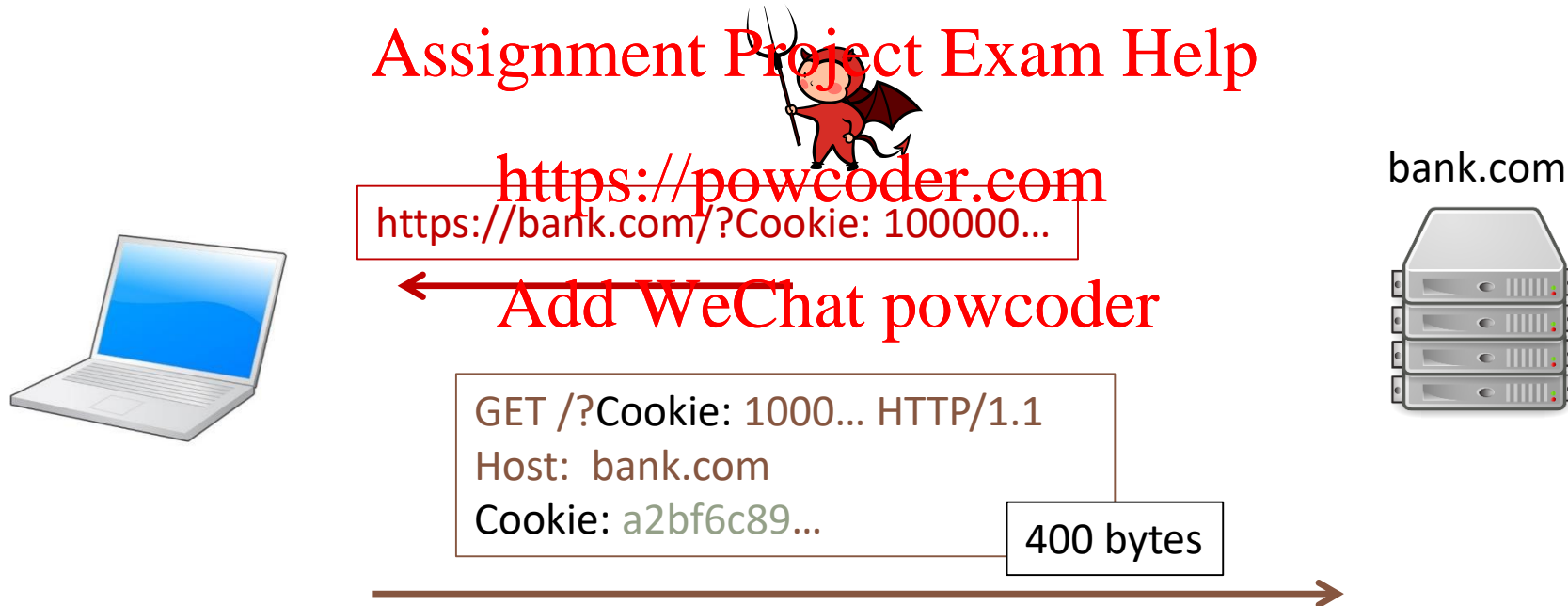
Discovered by Thai Duong and Juliano Rizzo, 2012





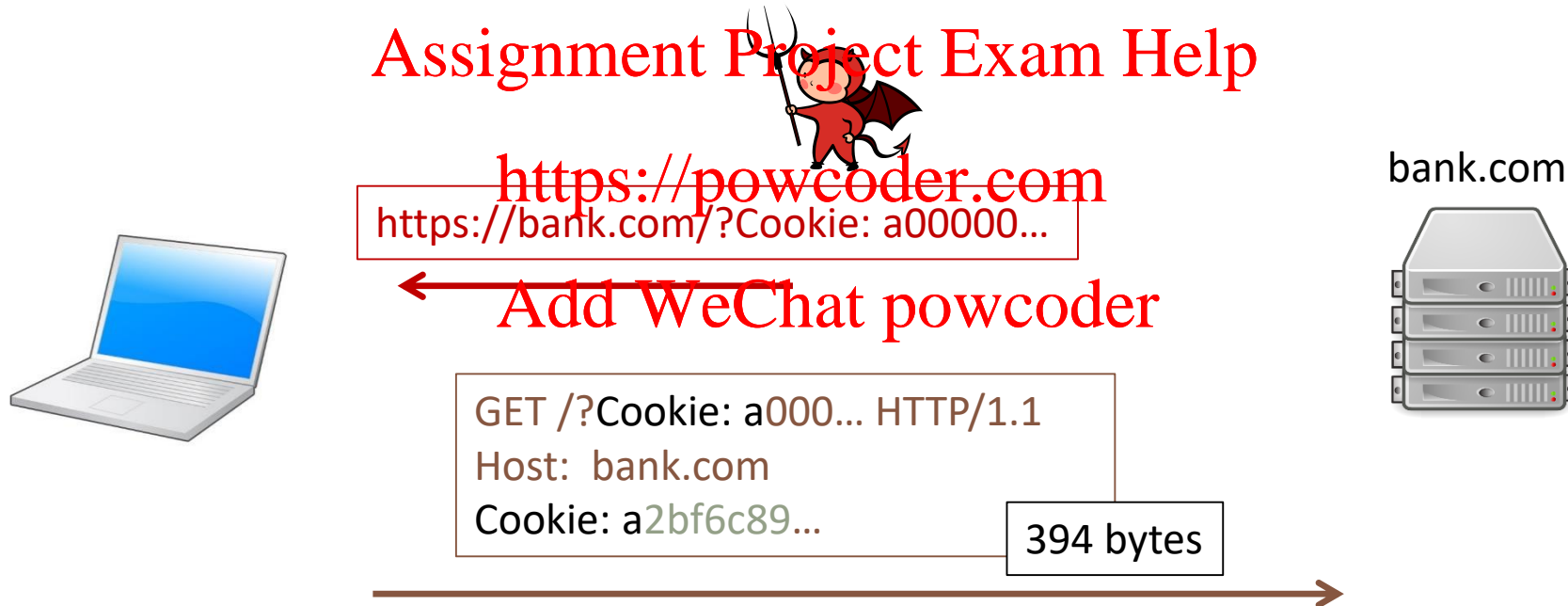
# CRIME attack

Discovered by Thai Duong and Juliano Rizzo, 2012



# CRIME attack

Discovered by Thai Duong and Juliano Rizzo, 2012



# CRIME attack

Discovered by Thai Duong and Juliano Rizzo, 2012



Assignment Project Exam Help

Guess

Request size

<https://powcoder.com>

Add WeChat powcoder

bank.com



000000...	400 bytes
100000...	400 bytes
200000...	400 bytes
...	
900000...	400 bytes
a00000...	<b>394 bytes</b>
b00000...	400 bytes

# goto fail;

---

```
hashOut.data = hashes + SSL_MD5_DIGEST_LEN;  
hashOut.length = SSL_SHA1_DIGEST_LEN;
```

2014 Apple TLS library – SSLVerifySignedServerKeyExchange()

```
if ((err = SSLFreeBuffer(&hashCtx)) != 0)  
    goto fail;
```

Assignment Project Exam Help

```
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)  
    goto fail;
```

<https://powcoder.com>

```
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)  
    goto fail;
```

```
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)  
    goto fail;
```

Add WeChat powcoder

```
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)  
    goto fail;  
goto fail;
```

```
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)  
    goto fail;
```

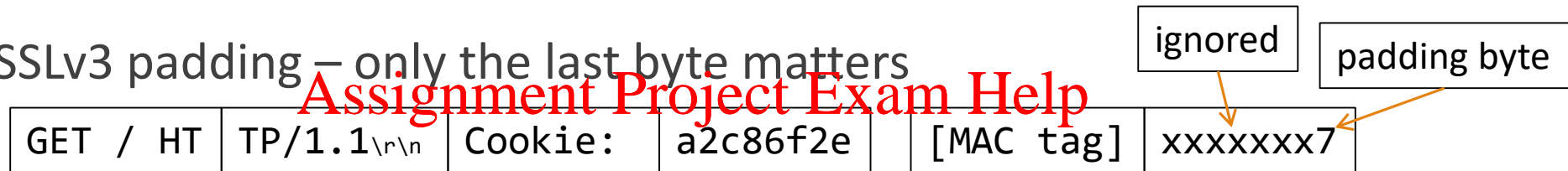
```
err = sslRawVerify(...);  
fail:  
    // Cleanup buffers, etc. Return err  
    return err;
```

# POODLE

Discovered by Bodo Möller, Thai Duong and Krzysztof Kotowicz, 2014

## Padding Oracle On Downgraded Legacy Encryption

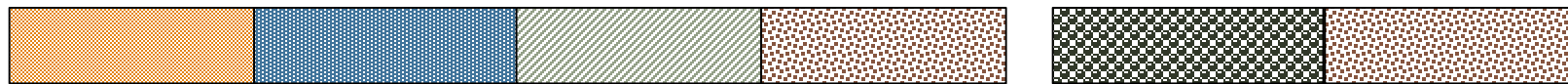
SSLv3 padding – only the last byte matters



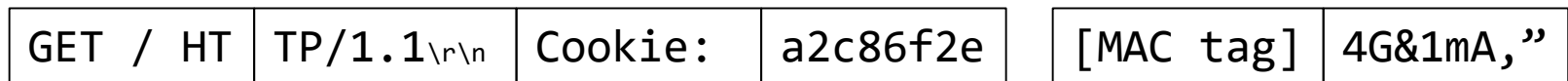
<https://powcoder.com>



Attacker copies cookie block to padding block



CBC Decrypt



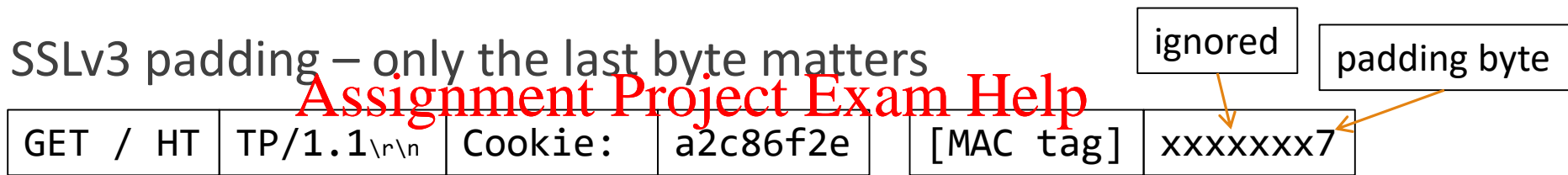
BAD PADDING OR MAC

# POODLE

Discovered by Bodo Möller, Thai Duong and Krzysztof Kotowicz, 2014

## Padding Oracle On Downgraded Legacy Encryption

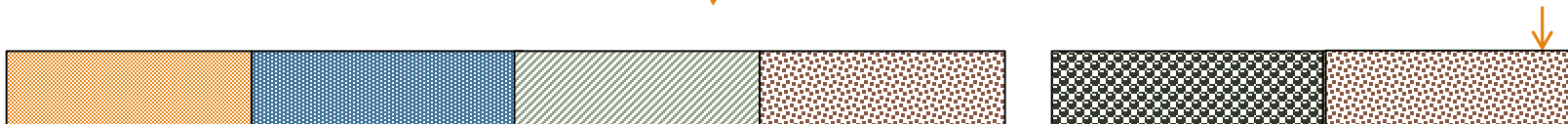
SSLv3 padding – only the last byte matters



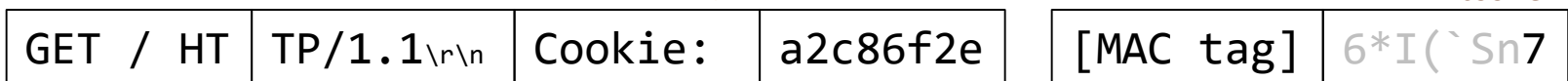
<https://powcoder.com>



Attacker copies cookie block to padding block



CBC Decrypt



$$P = D_K(C_{\text{cookie}}) \oplus C_{i-1}$$

Attacker learns last byte of  $D_K(C_{\text{cookie}})$ ! (shift cookie and repeat...)

Padding ignored;  
MAC OK



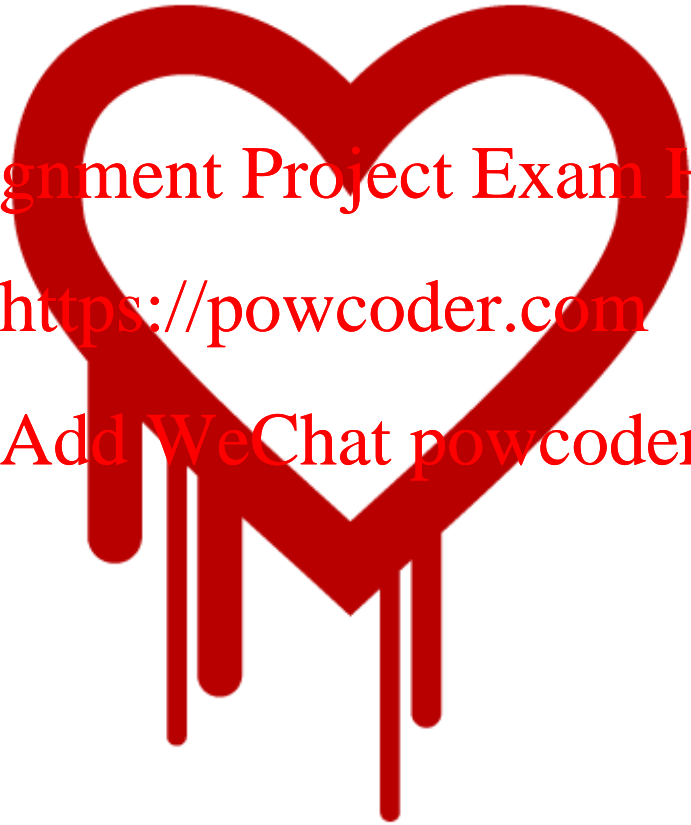
# Heartbleed

---

Assignment Project Exam Help

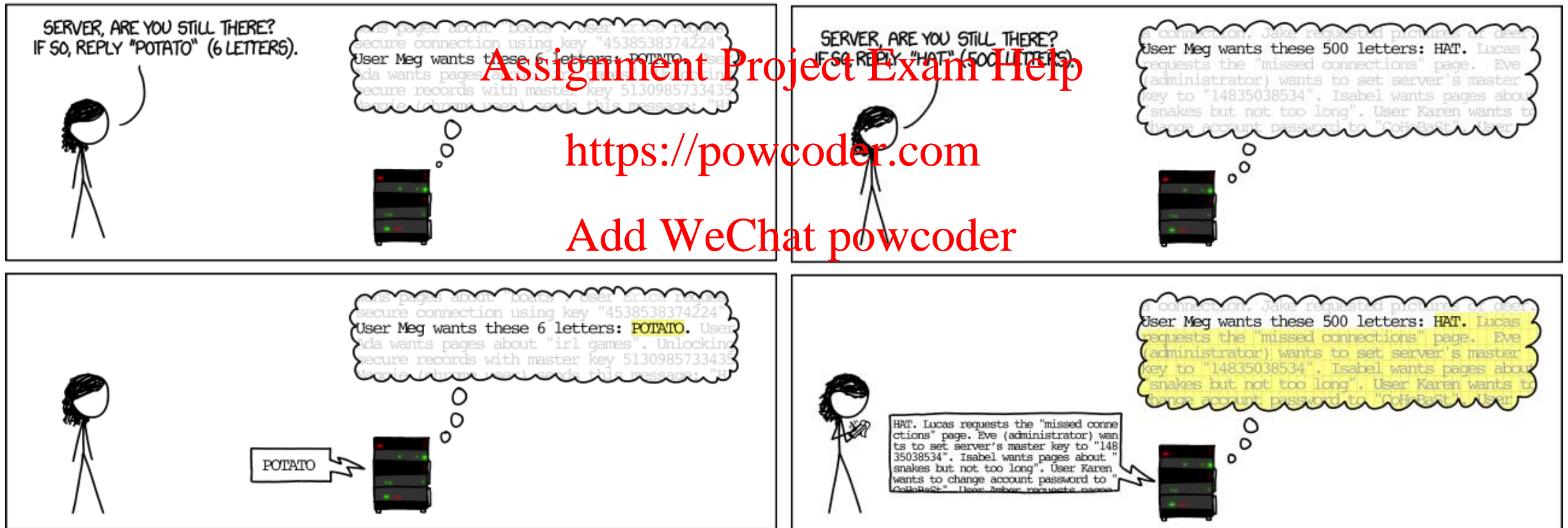
<https://powcoder.com>

Add WeChat powcoder



# Heartbleed

## HOW THE HEARTBLEED BUG WORKS:





# MD5 Considered Harmful Today

Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger

In 2008 (at CCC), a group of researchers showed that they could create a rogue CA certificate using an MD5 collision

serial number validity period	user prefix (difference)	rogue CA cert
real cert domain name		rogue CA RSA key
	collision bits (computed)	rogue CA X.509 extensions ← CA bit!
real cert RSA key		Netscape Comment Extension (contents ignored by browsers)
X.509 extensions	identical bytes (copied from real cert)	
signature		signature

# MD5 Considered Harmful Today

Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger

This kind of md5 collisions takes a bit more processing than `fastcoll` from the crypto project...

- So researchers used a cluster of 200 P3s for 12 days.
- Took 4 attempts (CA signatures)

<https://powcoder.com>

Add WeChat powcoder



# “Mining Your Ps and Qs”

Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman

In 2012, a team of researchers performed a global analysis of SSL/TLS and SSH keys

- 5.6% of TLS and 9.6% of SSH hosts shared cryptographic keys in a vulnerable manner
- Calculated the private keys for 0.5% of TLS hosts and 1.06% of SSH hosts
  - What if two RSA servers generate the same  $p$  but different  $q$ ?  $N_1 = pq_1$  and  $N_2 = pq_2$  [Find  $p$  given  $N_1$  and  $N_2$ ?]
- Uncovered vulnerabilities in Linux’s Random Number Generator (`/dev/urandom`)

