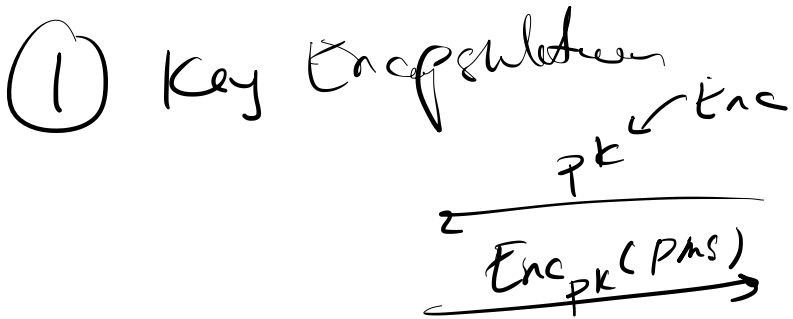
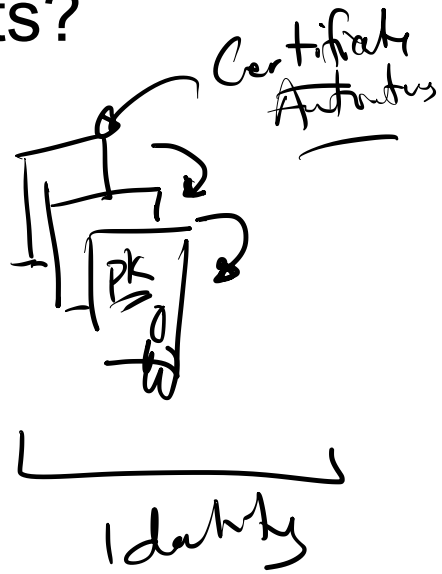
CS558 Network Security

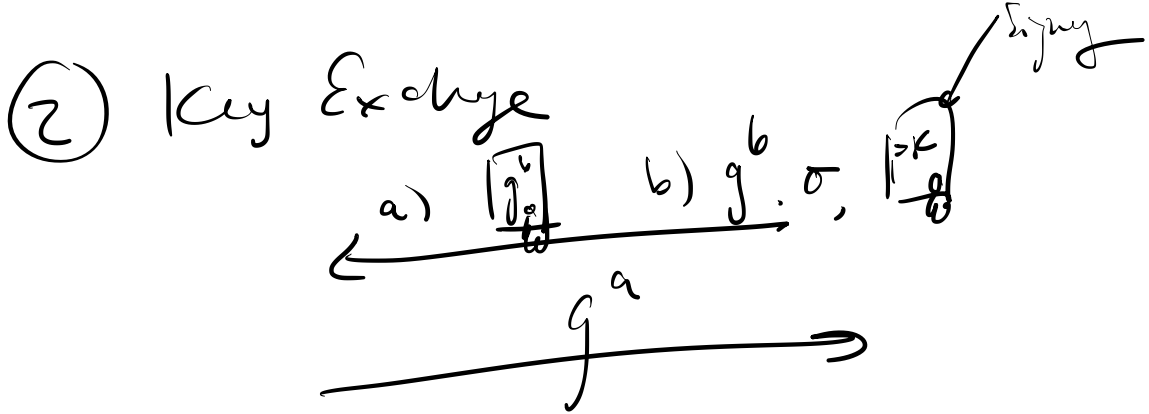
Lecture 13: Breaking TLS1.2 (and older)

BOSTON UNIVERSITY

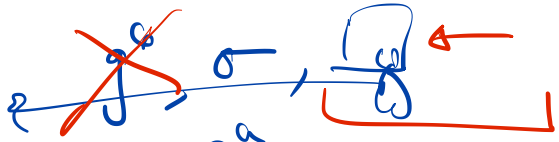
High Level Review -- What are the key parts?







TLS(1.2) in Detail



RFC 5246 TLS August 2008

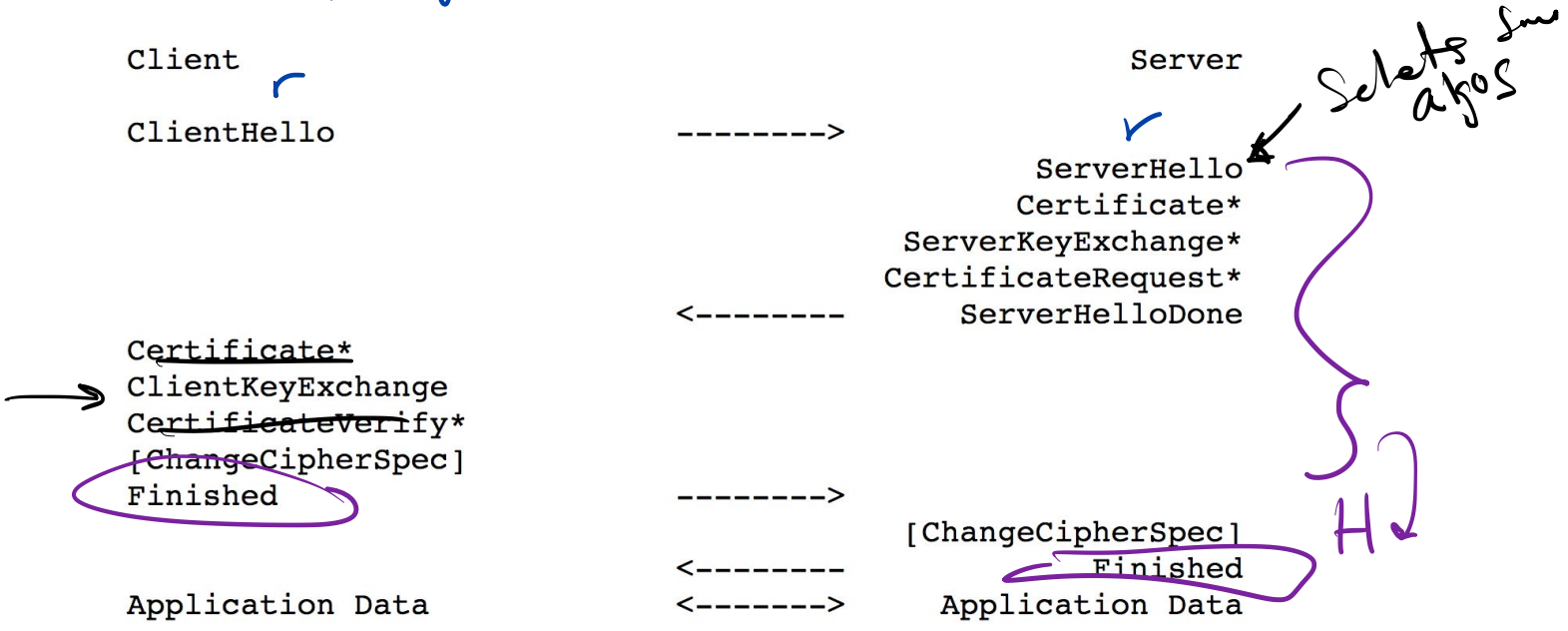


Figure 1. Message flow for a full handshake

Replay Attacks & Perfect Forward Secrecy

randomized transcripts from client and server

the ability to delete info

Emphemeral DH has PFS

Static DH + KEncap fail

Bleichenbacher's Attack (The Million Message Attack)

PKCS#1 v1.5

$m \longrightarrow c = m^e \bmod n$ (d)

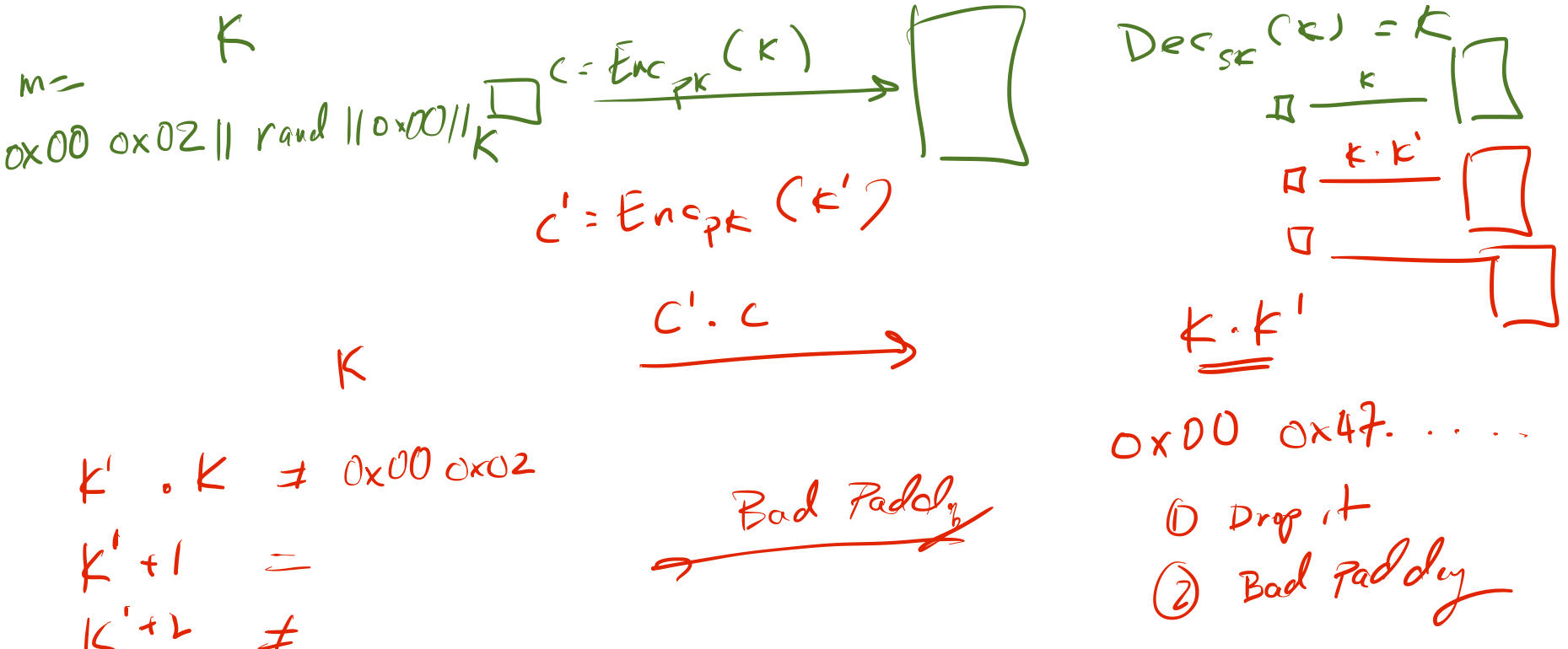
$d \equiv e^{-1} \bmod n$

$c^d = (m^e)^d = m^{ed} = m^1 \bmod n$

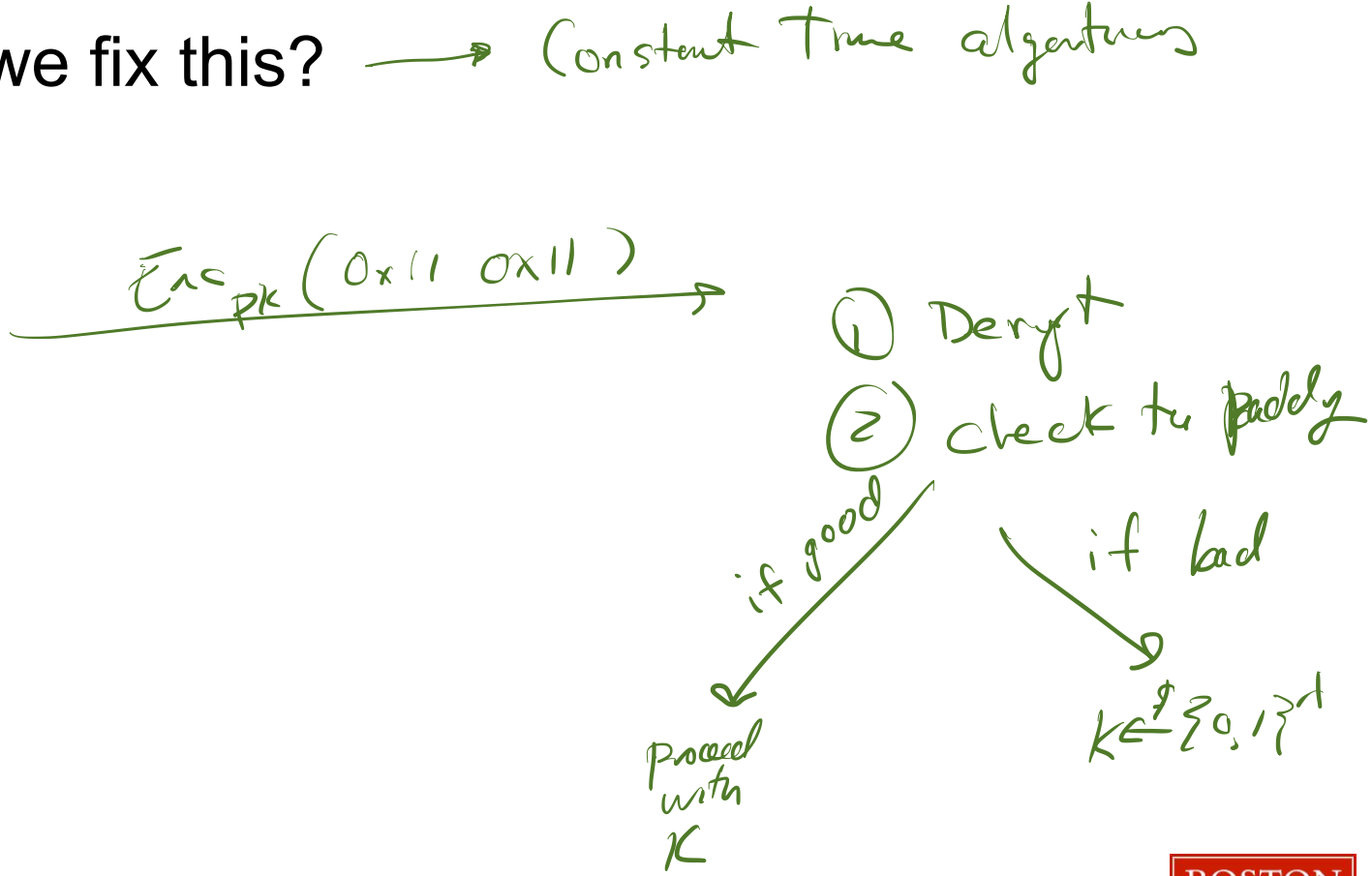
$c' = s^e \bmod n$

$c' \cdot c = m^e \cdot s^e = (m \cdot s)^e \bmod$

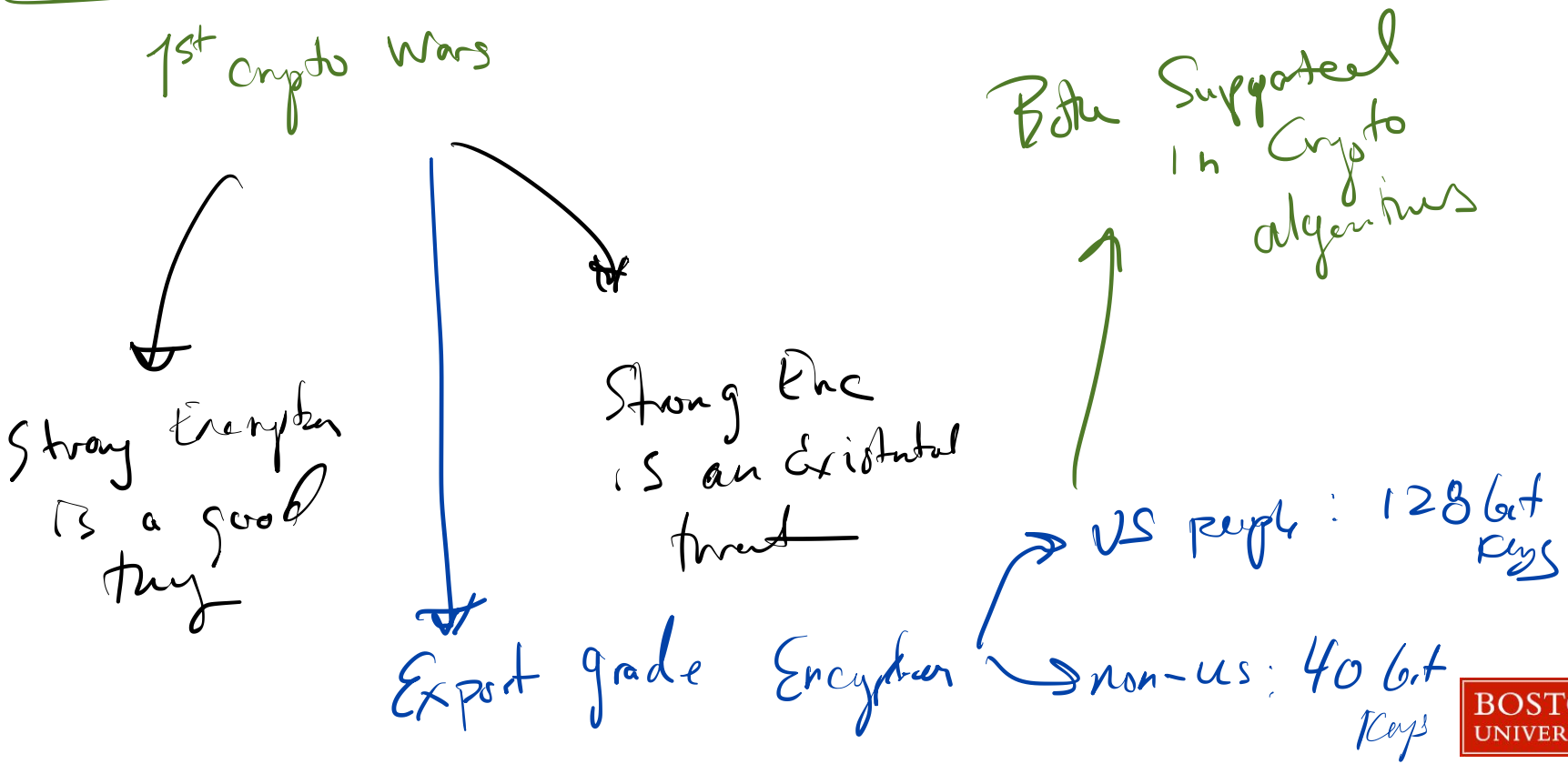
$Enc_{PK}(m) \cdot Enc_{PK}(s) = Enc_{PK}(m \cdot s)$

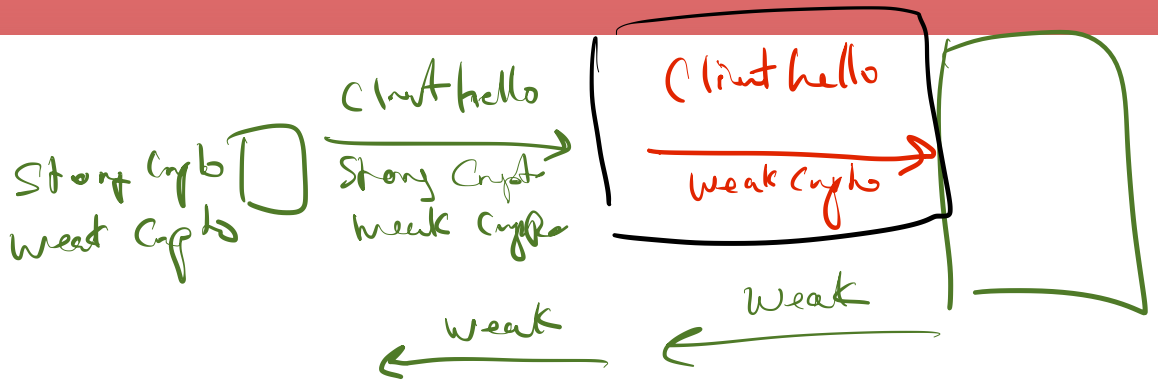


How should we fix this?



Downgrade Attacks





40 9 6

RSA - 2048

RSA - 512

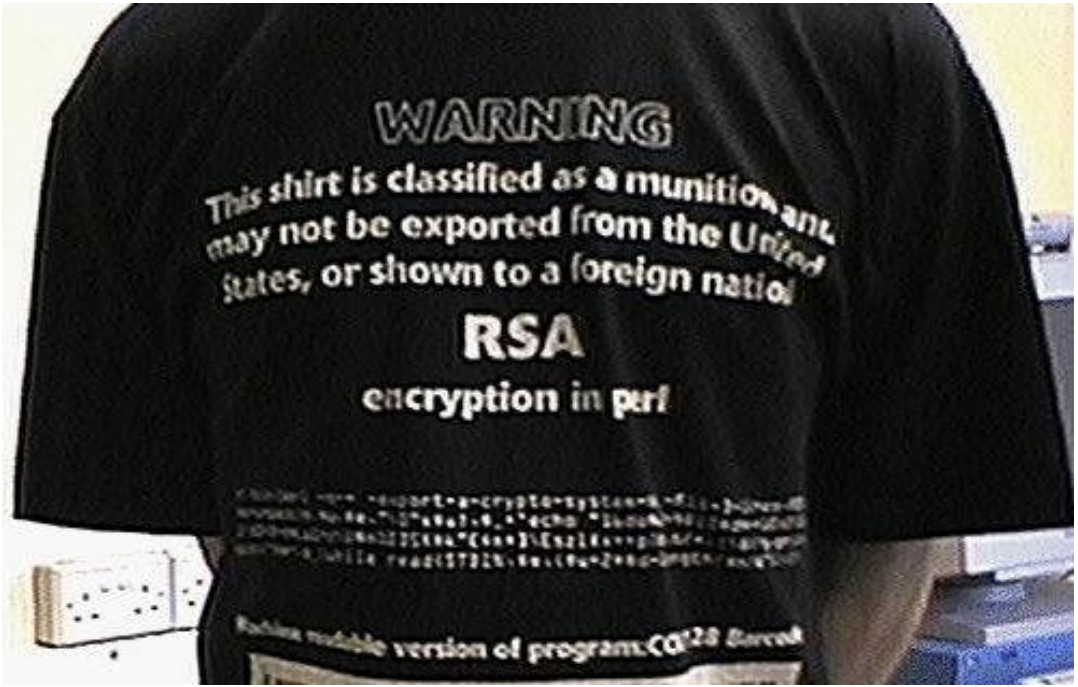
Problem :

(1) Existence of old ciphers

(2) Backwards Compatibility

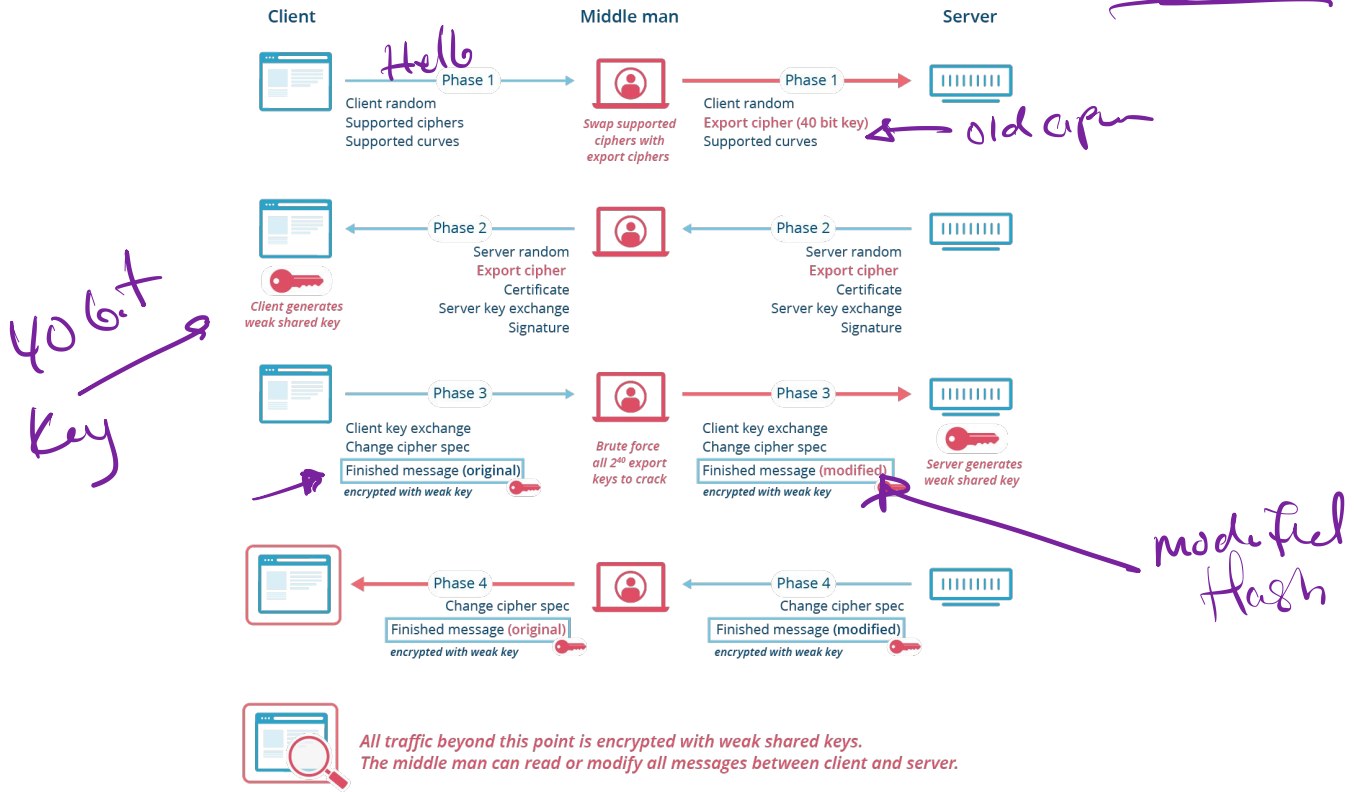
TLS_RSA_WITH_NULL_SHA256	NULL-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	DH-RSA-AES128-SHA256
TLS_DH_RSA_WITH_AES_256_CBC_SHA256	DH-RSA-AES256-SHA256
TLS_DH_RSA_WITH_AES_128_GCM_SHA256	DH-RSA-AES128-GCM-SHA256
TLS_DH_RSA_WITH_AES_256_GCM_SHA384	DH-RSA-AES256-GCM-SHA384
TLS_DH_DSS_WITH_AES_128_CBC_SHA256	DH-DSS-AES128-SHA256
TLS_DH_DSS_WITH_AES_256_CBC_SHA256	DH-DSS-AES256-SHA256
TLS_DH_DSS_WITH_AES_128_GCM_SHA256	DH-DSS-AES128-GCM-SHA256
TLS_DH_DSS_WITH_AES_256_GCM_SHA384	DH-DSS-AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	DHE-DSS-AES128-SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	DHE-DSS-AES256-SHA256
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	DHE-DSS-AES128-GCM-SHA256
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	DHE-DSS-AES256-GCM-SHA384
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	ECDH-RSA-AES128-SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	ECDH-RSA-AES256-SHA384
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	ECDH-RSA-AES128-GCM-SHA256
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	ECDH-RSA-AES256-GCM-SHA384
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	ECDH-ECDSA-AES128-SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	ECDH-ECDSA-AES256-SHA384
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	ECDH-ECDSA-AES128-GCM-SHA256
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	ECDH-ECDSA-AES256-GCM-SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
TLS_DH_anon_WITH_AES_128_CBC_SHA256	ADH-AES128-SHA256
TLS_DH_anon_WITH_AES_256_CBC_SHA256	ADH-AES256-SHA256
TLS_DH_anon_WITH_AES_128_GCM_SHA256	ADH-AES128-GCM-SHA256
TLS_DH_anon_WITH_AES_256_GCM_SHA384	ADH-AES256-GCM-SHA384

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html


WARNING
This shirt is classified as a munition and
may not be exported from the United
States, or shown to a foreign nation
RSA
encryption in perl

Downgrade Attack (FREAK)

(+Logjam Attack)



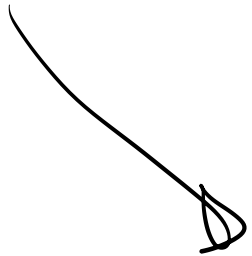
CLOUDFLARE

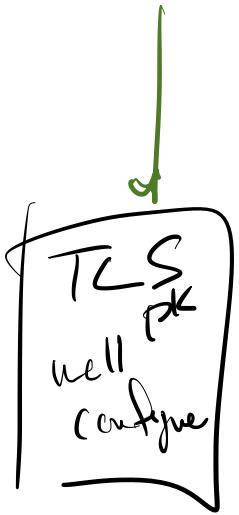
BOSTON UNIVERSITY

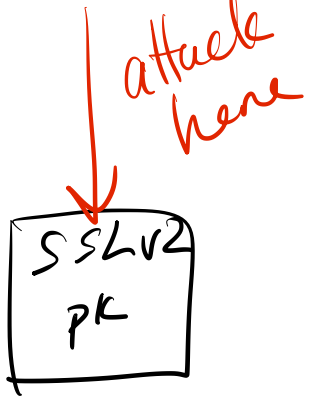
DROWN and ROBOT

↳ SSLv2
Brute force keys

↳ Bleichenbacher



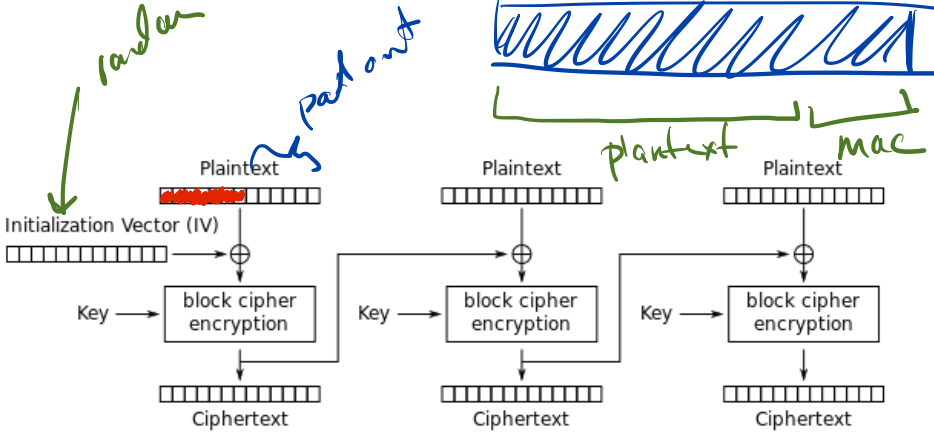




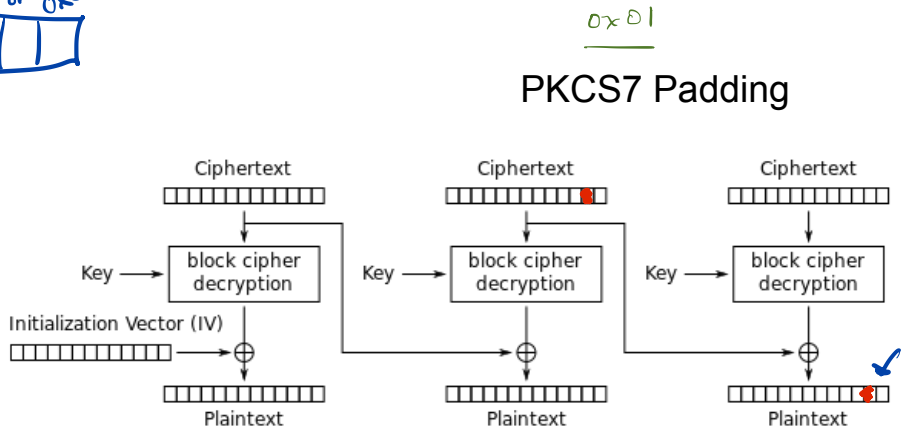
How should we fix this?

Break backwards compatibility

Padding Oracles in Symmetric Key Land (BEAST)

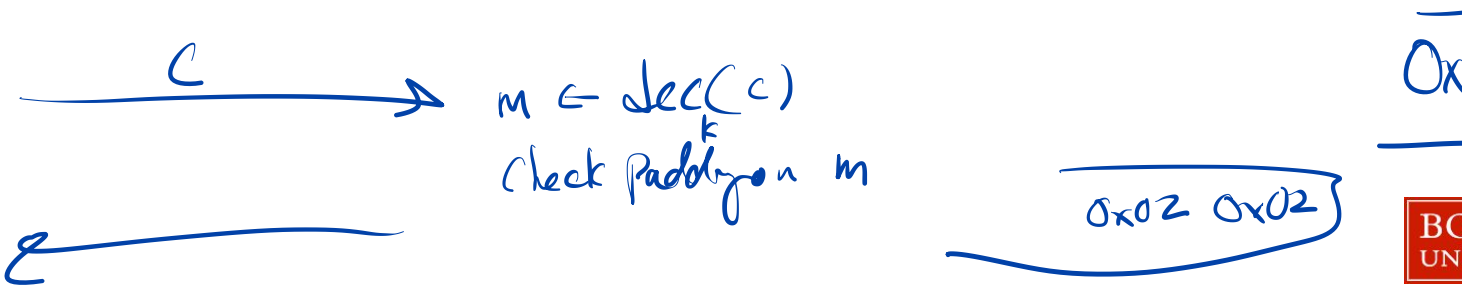


Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

PKCS7 Padding



BOSTON UNIVERSITY

TLS 1.2

MAC+Enc

TLS 1.3

Enc + MAC

X - A = 0x01

→ 0x01 - (0x07 + 0xFF)

0x08

How should we fix this?