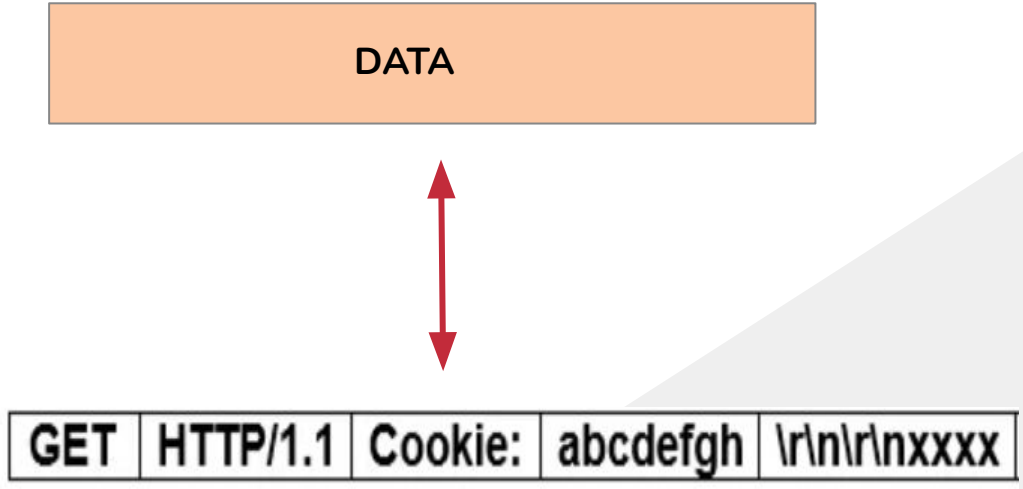
université de BORDEAUX

Lucky Thirteen & Poodle

Auteurs :

Hanane BENARAB
Youssef LACHABI
Alexandre ROSE

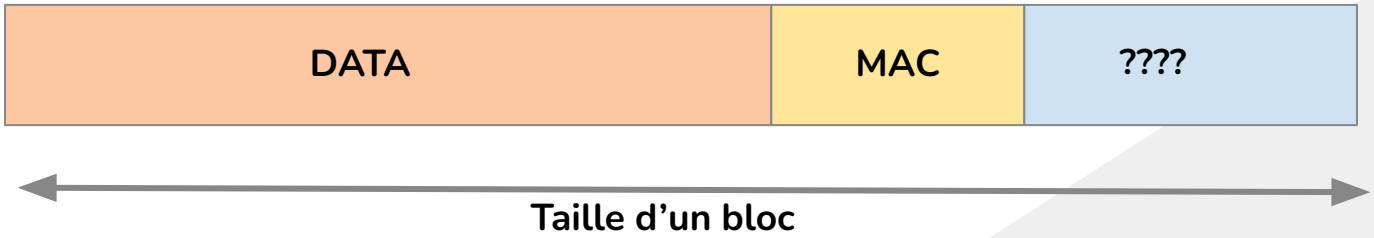
Padding :



Padding :

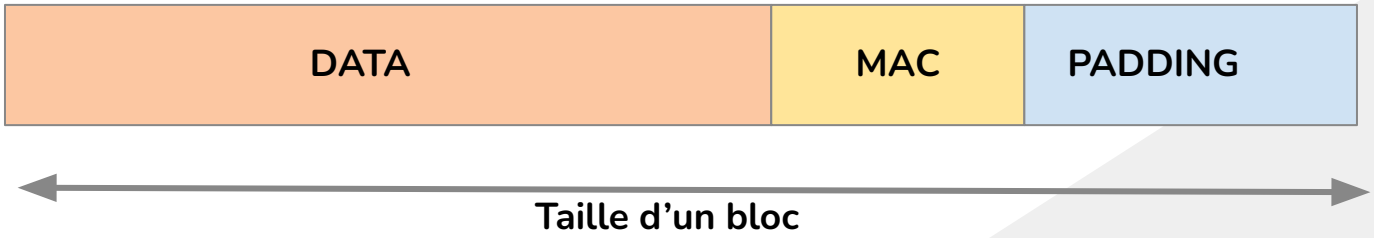
GET	HTTP/1.1	Cookie:	abcdefgh	\r\n\r\nxxxx

Padding :

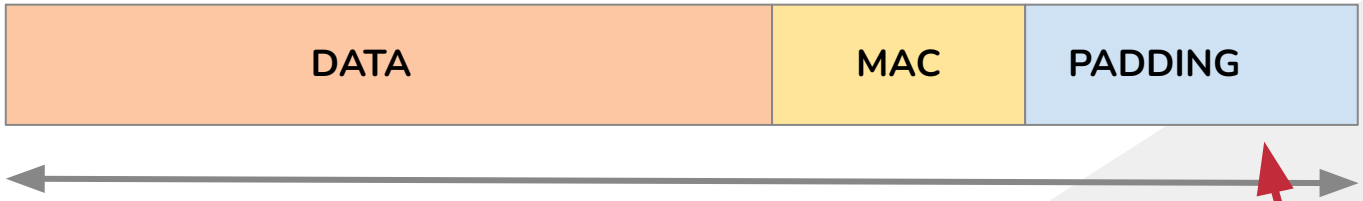


Et si la longueur du message n'est pas un multiple de la taille du bloc ??

Padding :



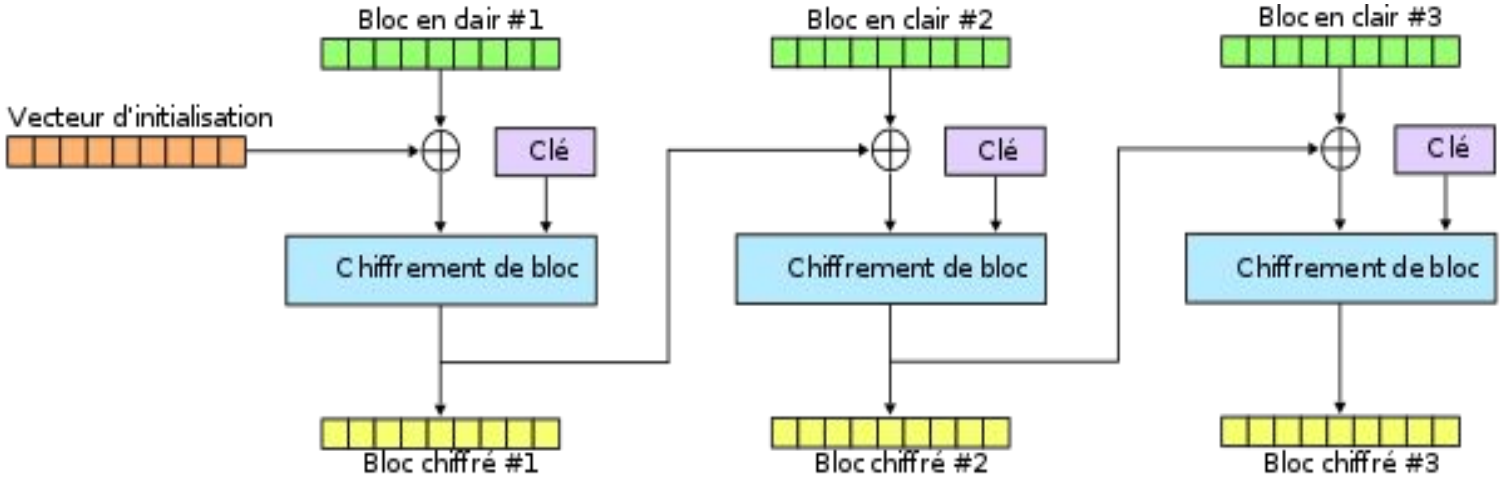
Norme PKCS #7 (RFC5652) :



Example : La taille d'un bloc == 08 Octets

H	E	L	L	O	0x03	0x03	0x03

CIPHER BLOC CHAINING (CBC) :



Chiffrement :

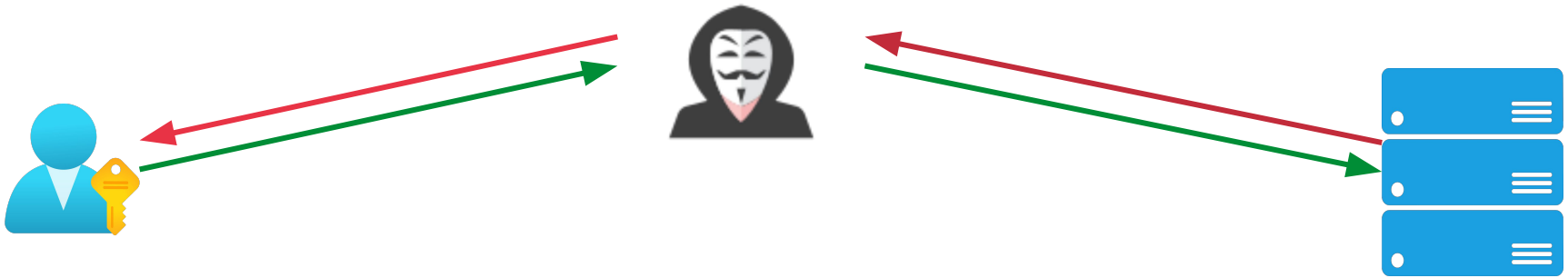
$$C_i = E_K(B_i \oplus C_{i-1})$$

Déchiffrement :

$$B_i = D_K(C_i) \oplus (C_{i-1})$$

Poodle attack

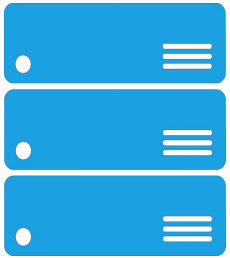
MITM attaque :



1) **Interception des messages chiffrés envoyés.**
2) **Down grade dance:**
   Forcer l'utilisation d'une version plus ancienne du protocole TLS ou SSL.

Côté serveur:

$$B_i = D_K(C_i) \oplus (C_{i-1})$$



C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8

Dk(_)

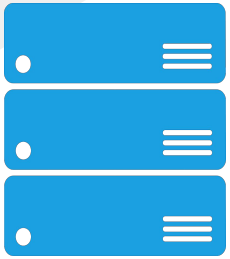
Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8

XOR

C1 :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	C1_8

M2 :	M2_1	M2_2	M2_3	M2_4	M2_5	M2_6	M2_7	M2_8

Côté serveur:



M2 : | M2_1 | M2_2 | M2_3 | M2_4 | M2_5 | M2_6 | M2_7 | M2_8 |

Padding correcte

X	X	X	X	X	X	X	1
X	X	X	X	X	X	2	2
8	8	8	8	8	8	8	8

Vérification du MAC

Padding incorrecte

X	X	X	X	X	X	1	2
X	X	X	X	X	2	3	2
X	X	X	X	X	X	X	%

Renvoie ‘ invalid padding ‘

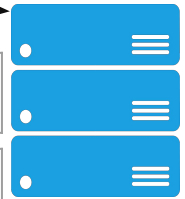
Côté attaquant:

C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1 :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	C1_8
IV :	IV1	IV2	IV3	IV4	IV5	IV6	IV7	IV8

M2 :								

Côté attaquant:

C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	0

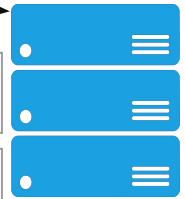


Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	0

Resultat:								

Côté attaquant:

C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	0

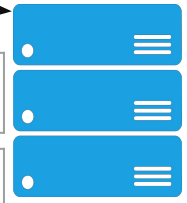


Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	0

Resultat:	X	X	X	X	X	X	X	#

Côté attaquant:

C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	0



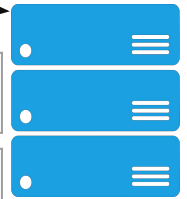
Invalid padding

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	0

Resultat:	X	X	X	X	X	X	X	#

Côté attaquant:

C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	1

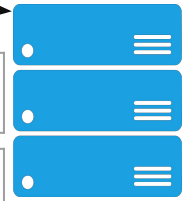


Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	1

Resultat:	X	X	X	X	X	X	X	13

Côté attaquant:

C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	1



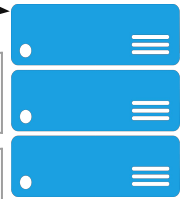
Invalid padding

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	1

Resultat:	X	X	X	X	X	X	X	13

Côté attaquant:

C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

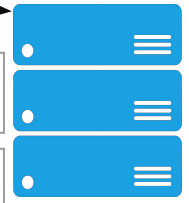


Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

Resultat:	X	X	X	X	X	X	X	01

Côté attaquant:

C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

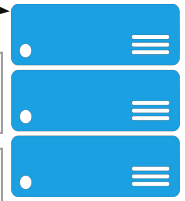


Invalid MAC

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N
Resultat:	X	X	X	X	X	X	X	01

Côté attaquant:

C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N



$X8 \oplus N = 01$

$X8 = 01 \oplus N$

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

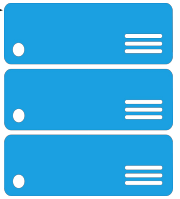
Resultat:	X	X	X	X	X	X	X	01

Côté attaquant:

Dk(C2) :								01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

X8 ⊕ N = 01

X8 = 01 ⊕ N



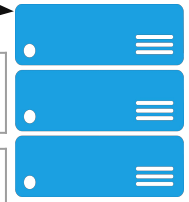
Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

Resultat:	X	X	X	X	X	X	X	01

Côté attaquant:

M2:								
Dk(C2) :								01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

M2_8 = Dk(C2_8) ⊕ C1_8



Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

Resultat:	X	X	X	X	X	X	X	01

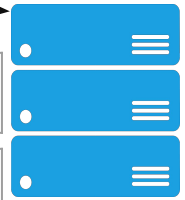
Côté attaquant:

M2:								03
Dk(C2) :								01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

M2_8 = Dk(C2_8) ⊕ C1_8

M2_8 = 03

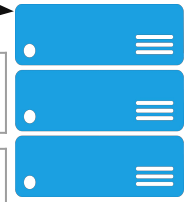
Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N



Resultat:	X	X	X	X	X	X	X	01

Côté attaquant:

M2:								03
Dk(C2) :								01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

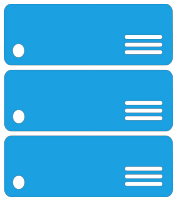


Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	N

Resultat:	X	X	X	X	X	X	X	01

Côté attaquant:

M2:								03
Dk(C2) :								01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	Z1	Z2



Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	Z1	Z2
Resultat:	X	X	X	X	X	X	02	02

Côté attaquant:

M2:								03
Dk(C2) :								01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	Z1	X8 ⊕ 02

X8 ⊕ Z2 = 02
Z2 = X8 ⊕ 02

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	Z1	X8 • 02
Resultat:	X	X	X	X	X	X	02	02

Côté attaquant:

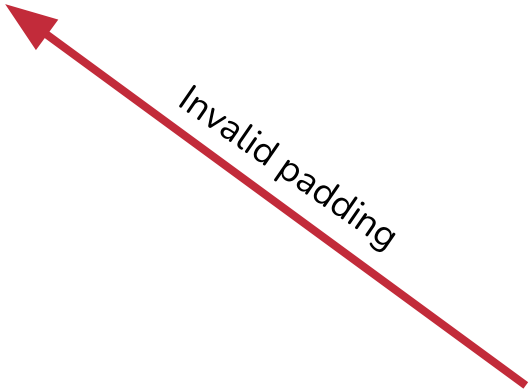
M2:								03
Dk(C2) :								01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	0	X8 ⊕ 02

Invalid padding

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	0	X8 • 02
Resultat:	X	X	X	X	X	X	(	02

Côté attaquant:

M2:								03
Dk(C2) :								01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	01	X8 ⊕ 02



Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	01	X8 • 02
Resultat:	X	X	X	X	X	X	09	02

Côté attaquant:

M2:								03
Dk(C2) :								01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	B	X8 ⊕ 02

Invalid MAC

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	B	X8 • 02
Resultat:	X	X	X	X	X	X	02	02

Côté attaquant:

M2:								03
Dk(C2) :								01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	B	X8 ⊕ 02

X7 ⊕ B = 02

X7 = 02 ⊕ B
M2_7 = X7 ⊕ C1_7
M2_7 = 03

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	B	X8 • 02
Resultat:	X	X	X	X	X	X	02	02

Côté attaquant:

M2:							03	03
Dk(C2) :							02 ⊕ B	01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	B	X8 ⊕ 02

X7 ⊕ B = 02

X7 = 02 ⊕ B
M2_7 = X7 ⊕ C1_7
M2_7 = 03

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	B	X8 • 02
Resultat:	X	X	X	X	X	X	02	02

Côté attaquant:

M2:							03	03
Dk(C2) :							02 ⊕ B	01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1' :	C1_1	C1_2	C1_3	C1_4	C1_5	Z1	Z2	Z3

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1':	C1_1	C1_2	C1_3	C1_4	C1_5	Z1	Z2	Z3
Resultat:	X	X	X	X	X	03	03	03

Côté attaquant:

M2:	H	E	L	L	O	03	03	03
Dk(C2) :	12 ⊕ L	06 ⊕ F	17 ⊕ K	05 ⊕ P	63 ⊕ N	05 ⊕ K	02 ⊕ B	01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1 :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	C1_8

Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1:	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	C1_8

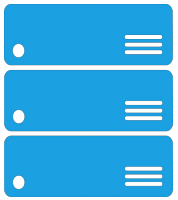
Resultat:	H	E	L	L	O	03	03	03

Côté attaquant:

M2:	H	E	L	L	O	03	03	03
Dk(C2) :	12 ⊕ L	06 ⊕ F	17 ⊕ K	05 ⊕ P	63 ⊕ N	05 ⊕ K	02 ⊕ B	01 ⊕ N
C2 :	C2_1	C2_2	C2_3	C2_4	C2_5	C2_6	C2_7	C2_8
C1 :	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	C1_8

(C1 ; C2) <- (IV ; C1)

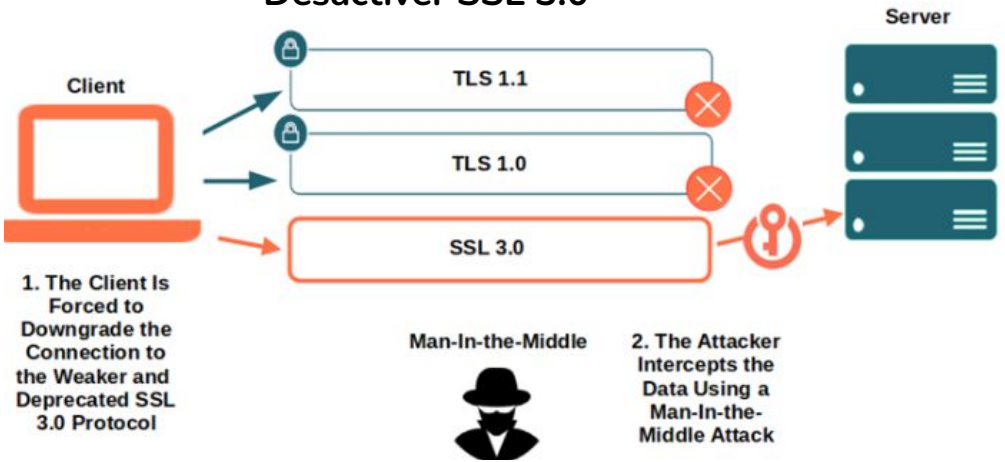
Dk(C2):	X1	X2	X3	X4	X5	X6	X7	X8
C1:	C1_1	C1_2	C1_3	C1_4	C1_5	C1_6	C1_7	C1_8



Resultat:	H	E	L	L	O	03	03	03

Correctif de Poodle: solution évidente ?

Désactiver SSL 3.0



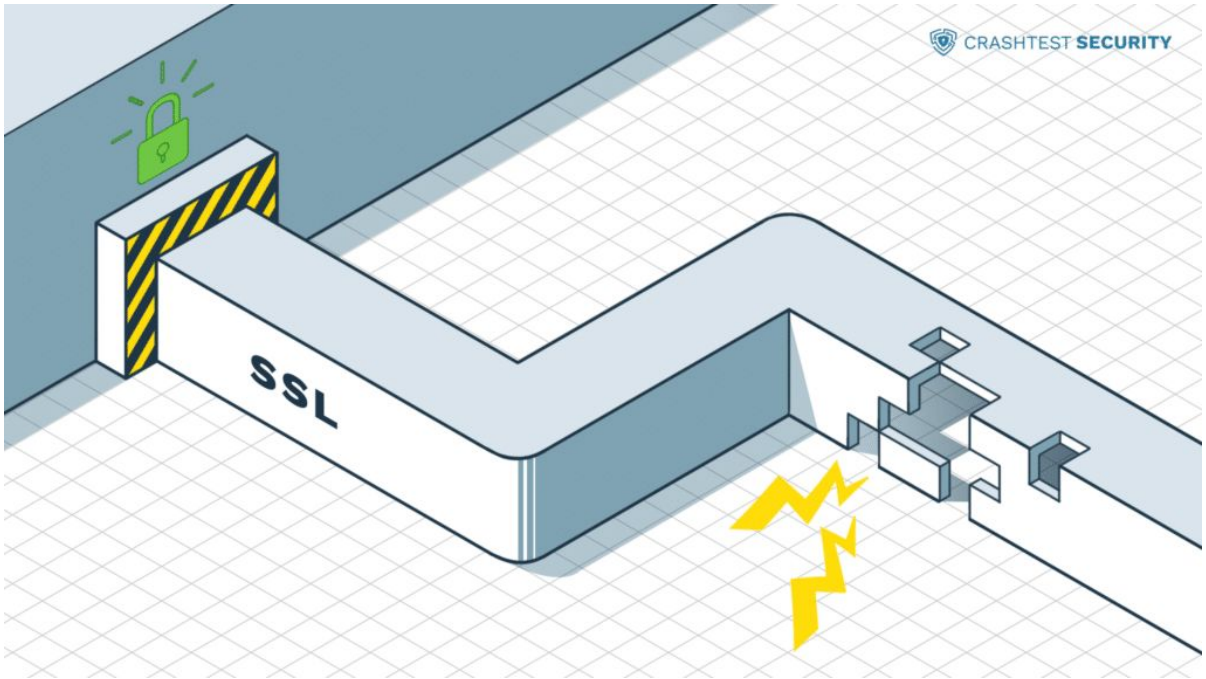
Problème de compatibilité:

- Nombreux sites impactés
- Legacy systems

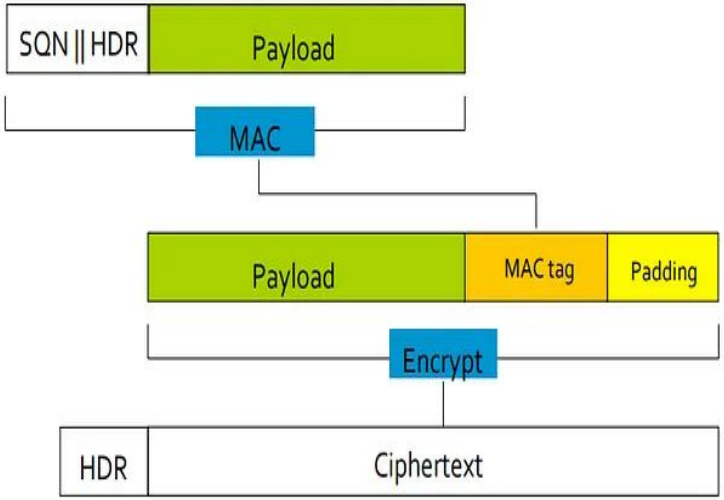
Enlever les chiffrements en mode CBC vulnérables ?

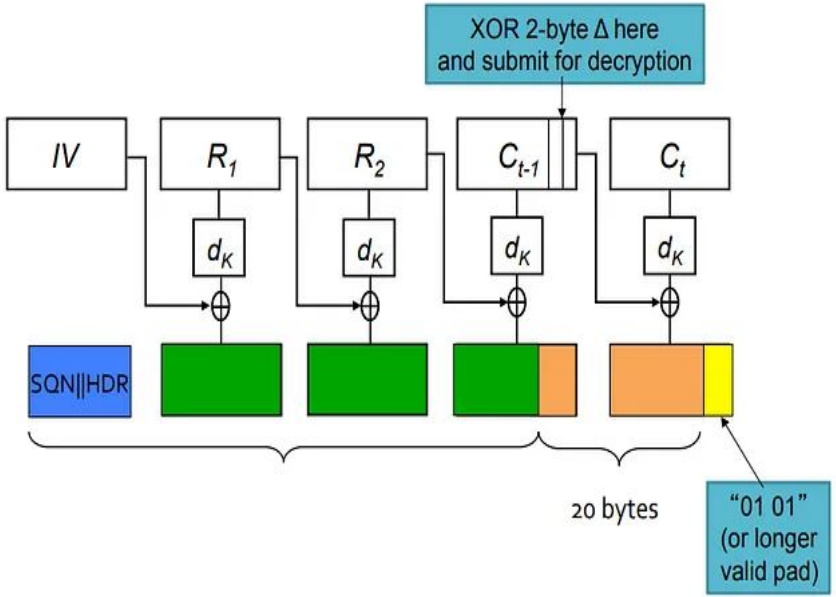
RC4 vulnérable

Correctif de Poodle: TLS_FALLBACK_SCSV

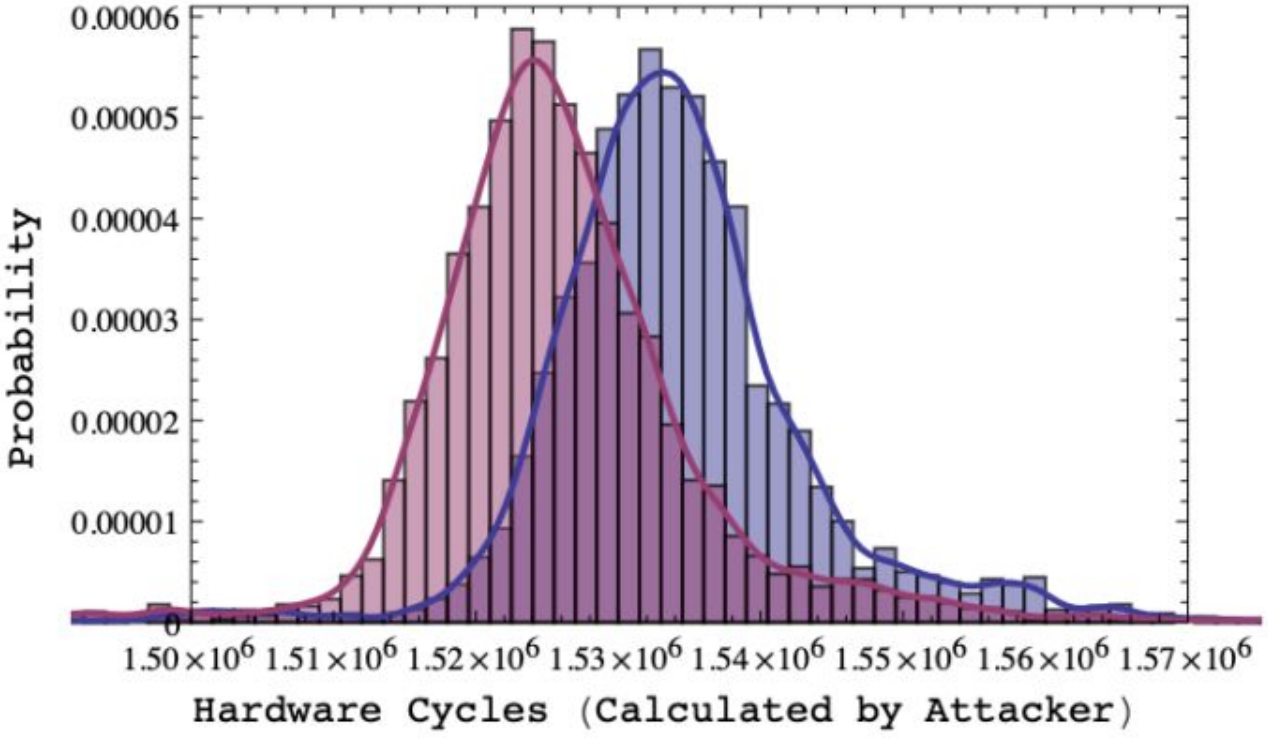


Lucky 13: a cryptographic timing attack:



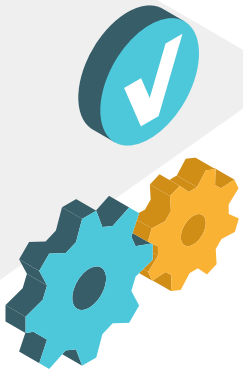


Lucky 13: a cryptographic timing attack:



Bon Padding
+ MAC invalide

MAC invalide
+ Padding invalide



MERCI DE VOTRE ATTENTION