MATH 178 Homework #9

Tamir Enkhjargal

May 2019

AES

5.

First we will need to expand the key we are given: `1100 1011 1111 1110`

$$
\begin{aligned}
W[0] &= \texttt{1100 1011} && (1)\\
W[1] &= \texttt{1111 1110} && (2)\\
W[2] &= W[0] \oplus RCON(1) \oplus Sub(Rot(W[1])) && (3)\\
&= Rot(W[1]) = \texttt{1110 1111} && (4)\\
&= Sub(Rot(W[1])) = \texttt{1111 0111} && (5)\\
&= 11110111 \oplus 10000000 \oplus 11001011 && (6)\\
W[2] &= \texttt{1011 1100} && (7)\\
W[3] &= W[1] \oplus W[2] && (8)\\
&= 11111110 \oplus 10111100 && (9)\\
W[3] &= \texttt{0100 0010} && (10)\\
W[4] &= W[2] \oplus RCON(2) \oplus Sub(Rot(W[3])) && (11)\\
&= Rot(W[3]) = \texttt{0010 0100} && (12)\\
&= Sub(Rot(W[3])) = \texttt{1010 1101} && (13)\\
&= 10101101 \oplus 00110000 \oplus 10111100 && (14)\\
W[4] &= \texttt{0010 0001} && (15)\\
W[5] &= W[3] \oplus W[4] && (16)\\
&= 01000010 \oplus 00100001 && (17)\\
W[5] &= \texttt{0110 0011} && (18)\\
K_0 &= \texttt{1100 1011 1111 1110} && (19)\\
K_1 &= \texttt{1011 1100 0100 0010} && (20)\\
K_2 &= \texttt{0010 0001 0110 0011} && (21)
\end{aligned}
$$

Now, we can use CBC alongside Simplified AES. The initialization vector XOR'ed with our PT_1 is `0100001101001111`$\oplus$`1000110100001011`=`1100111001000100`. As a reminder simplified AES goes like:

$$A_{K2} \circ SR \circ NS \circ A_{K1} \circ MC \circ SR \circ NS \circ A_{K0}$$

$$
\begin{aligned}
CT_1 &= CT_0 \oplus K_0 && (1)\\
&= 1100111001000100 \oplus 1100101111111110 && (2)\\
CT_1 &= \texttt{0000 0101 1011 1010} && (3)\\
CT_2 &= NS(CT_1) && (4)\\
CT_2 &= \texttt{1001 0001 0011 0000} && (5)\\
CT_3 &= SR(CT_2) && (6)
\end{aligned}
$$

$$CT_3 = \texttt{1001 0000 0011 0001} \quad (7)$$
$$CT_4 = MC(CT_3) \quad (8)$$
$$CT_4 = \texttt{1001 0010 0111 1101} \quad (9)$$
$$CT_5 = CT_4 \oplus K_1 \quad (10)$$
$$= 1001001001111101 \oplus 1011110001000010 \quad (11)$$
$$CT_5 = \texttt{0010 1110 0011 1111} \quad (12)$$
$$CT_6 = NS(CT_5) \quad (13)$$
$$CT_6 = \texttt{1010 1111 1011 0111} \quad (14)$$
$$CT_7 = SR(CT_6) \quad (15)$$
$$CT_7 = \texttt{1010 0111 1011 1111} \quad (16)$$
$$CT_8 = CT_7 \oplus K_2 \quad (17)$$
$$= 1010011110111111 \oplus 0010000101100011 \quad (18)$$
$$CT_8 = \texttt{1000 0110 1101 1100} \quad (19)$$

Our final ciphertext from the first round in CBC is 1000011011011100. XOR'ing the CT and the PT_2 will get us the "initialization".

$$1000011011011100 \oplus 0100010101001110 = \texttt{1100 0011 1001 0010}$$

$$CT_1 = CT_0 \oplus K_0 \quad (1)$$
$$= 1100001110010010 \oplus 1100101111111110 \quad (2)$$
$$CT_1 = \texttt{0000 1000 0110 1100} \quad (3)$$
$$CT_2 = NS(CT_1) \quad (4)$$
$$CT_2 = \texttt{1001 0110 1000 1100} \quad (5)$$
$$CT_3 = SR(CT_2) \quad (6)$$
$$CT_3 = \texttt{1001 1100 1000 0110} \quad (7)$$
$$CT_4 = MC(CT_3) \quad (8)$$
$$CT_4 = \texttt{1100 1110 0011 0000} \quad (9)$$
$$CT_5 = CT_4 \oplus K_1 \quad (10)$$
$$= 1100111000110000 \oplus 1011110001000010 \quad (11)$$
$$CT_5 = \texttt{0111 0010 0111 0010} \quad (12)$$
$$CT_6 = NS(CT_5) \quad (13)$$
$$CT_6 = \texttt{0101 1010 0101 1010} \quad (14)$$
$$CT_7 = SR(CT_6) \quad (15)$$
$$CT_7 = \texttt{0101 1010 0101 1010} \quad (16)$$
$$CT_8 = CT_7 \oplus K_2 \quad (17)$$
$$= 0101101001011010 \oplus 0010000101100011 \quad (18)$$
$$CT_8 = \texttt{0111 1011 0011 1001} \quad (19)$$
$$CT_{total} = \texttt{1000 0110 1101 1100 0111 1011 0011 1011} \quad (20)$$

8.

i)

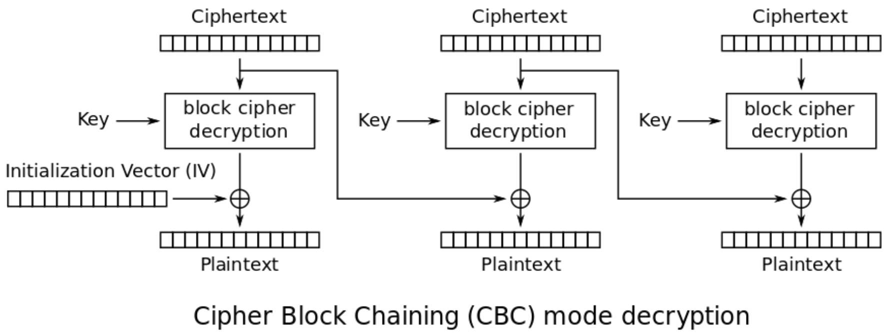

Figure 1: CBC decryption, as taken from Wikipedia

ii) Assuming both Alice and Bob have shared the same key and IV, when one-bit from the CT transfer is corrupted, as we saw from the diffusion example in class, the real AES will have enough rounds so that a single changed bit will affect all bits in the next CT/PT completely. Therefore, Bob would only be able to decrypt and get PT_1 to PT_3 correctly.

iii) Regardless of "nice" PT or "not nice" PT, it doesn't matter to the computer and AES. Bob will still only be able to determine PT_1 and PT_3 because the complete diffusion of the incorrect bit transferring into the next blocks.

NT

18.

Reduce $17^{53} \pmod{97}$

$b = 17,\ n = 43,\ m = 97,\ S[\ ] = \{1, 1, 0, 1, 0, 1\},\ k = 5$

$b(\text{mod}97)$	s	a
		1
17	s[0]=1	17
17^2=95	s[1]=0	17
95^2=4	s[2]=1	68
4^2=16	s[3]=0	68
16^2=62	s[4]=1	45
62^2=61	s[5]=1	29

LM

4.

The last four hex ciphertext is `9A3F`. Encrypting and decrypting using the same key gets me the plaintext back.