Cryptology Wk 5

1) a)

ti

b) given $A_{uuf\text{-}cma}$ that can
m^* is given and not possible to call $\mathcal{T}(m^*)$

$B^{\mathcal{T}(\cdot)}_{euf\text{-}cma}$

$\hat{m} \xleftarrow{\$} \mathcal{M} / \{m^*\}$

$\hat{t} \leftarrow A^{\mathcal{T}(\cdot)}(\hat{m})$

return $(\hat{m}, \hat{t})$

return

c) $t' = t$ $q' = q$ and $\varepsilon' = \varepsilon$

2) a) CBC-MAC encrypts the message under CBC-Mode block cipher and return the last encrypted block

b) $CFB.Mac_k(m[1], \dots, m[b])$

$c[1] \leftarrow m[1]$

for $i \in \{2, \dots, n\}$

$X[i] \leftarrow E_k(c[i-1])$

$c[i] \leftarrow m[i] \oplus X[i]$

return $E_k(c'[b])$

$c[1] \leftarrow m[1]$

$X[2] \leftarrow E_k(m[1])$

$c[2] \leftarrow m[2] \oplus E_k(m[1])$

$c[3] \leftarrow m[3] \oplus E_k(m[2] \oplus E_k(m[1]))$

$m[..] \oplus E_k(..)$

$E_k(m[..] \oplus E_k(..))$

returns $E_k(m[b] \oplus E_k(m[b-1] \oplus \dots \oplus E_k(m[2] \oplus E_k(m[1]))))$

$CBC.Mac_k(m[1], \dots, m[b])$

$X[0] \leftarrow 0^\ell$

for $i \in \{1, \dots, n\}$

$Y[i] \leftarrow X[i-1] \oplus m[i]$

$X[i] \leftarrow E_k(Y[i])$

return $X[b]$

$X[0] \leftarrow 0^\ell$

$X[1] \leftarrow E_k(m[1])$

$X[2] \leftarrow E_k(m[2] \oplus E_k($

$Y[1] \leftarrow m[1]$

$Y[2] \leftarrow m[2] \oplus E_k(m[1])$

$E_k(m[..] \oplus E_k(-))$

returns $E_k(m[b] \oplus E_k(m[b-1] \oplus \dots \oplus E_k(m[2] \oplus E_k(m[1]))$.

(3) a) $x[0] \leftarrow 0^\ell$

$y[1] \leftarrow x[0] \oplus m[0] = 0^\ell \oplus 0^\ell = 0^\ell$

$x[1] \leftarrow E_k(0^\ell)$

$t \leftarrow E_k(0^\ell)$

$0^\ell \| t$

$x[0] \leftarrow 0^\ell$

$y[1] \leftarrow 0^\ell \oplus m[0] = 0^\ell \oplus 0^\ell = 0^\ell$

$x[1] \leftarrow E_k(0^\ell)$

$y[2] \leftarrow x[1] \oplus m[1] = E_k(0^\ell) \oplus t = t \oplus t = 0^\ell$

$x[2] \leftarrow E_k(y[2]) = E_k(0^\ell) = t$

return $x[2] = t$

so t is also the tag for $0 \| t$

b) existential forgery

chosen message

c)

$y[b] \leftarrow x[b-1] \oplus m[b] =$

$x[b] \leftarrow E_k(y[b]) = t$

$y[b+1] \leftarrow x[b] \oplus t = t \oplus t = 0^\ell$

$x[b+1] \leftarrow E_k(y[b]) = x[$

$t = \mathrm{Tag}(0^\ell \| m[0] \| \ldots \| m[b])$

then $t = \mathrm{Tag}(0^\ell \| (m[0] \| \ldots \| m[b] \| t)^* (m[0] \| \ldots \| m[b]))$

$\rightarrow 0^{\ell}$

Cryptology Wk 5

$X[0] \leftarrow 0^{\ell}$

$Y[1] \leftarrow X[0] \oplus m[0] = 0^{\ell} \oplus m[0] = m[0]$

$X[1] \leftarrow E_K(m[0])$

$t \leftarrow E_K(m[0])$

$\rightarrow m[0] \| (m[0] \oplus t)$

$X[0] \leftarrow 0^{\ell}$

$Y[1] \leftarrow X[0] \oplus M[0] = 0^{\ell} \oplus m[0] = m[0]$

$X[1] \leftarrow E_K(Y[1]) = E_K(m[0]) = t$

$Y[2] \leftarrow X[1] \oplus m[1] = t \oplus (t \oplus m[0]) = m[0]$

$X[2] \leftarrow E_K(m[0]) = t$

$t = Tag_K(m[0] \| \dots \| m[b])$

then $Tag_K((m[0] \| \dots \| m[b] \| (m[0] \oplus t))^{*} (m[0] \| \dots \| m[b])) = t$ as well

d) - Immediatly by guessing the remaining $\ell - \tau$ bits there is a probability of $(\frac{1}{2})^{\ell-\tau}$ of using the length extension attack

- ~~The probability of Advantage of the adversary can be increased at the cost of additional queries to the oracle. This method would work by~~

- It is insecure under EUF-CMA-security if given reasonable $t \propto 2^{\ell-\tau}$ and $q \propto 2^{\ell-\tau}$ by trying each possible extension on a message of the form

$t \leftarrow Tag_K(m[0] \| \dots \| m[b])$ obtained via oracle

for i in $\{0, \dots, 2^{\ell-\tau}\}$

$\quad$ t_guess $\leftarrow tag_K((m[0] \| \dots \| m[b] \| (t \| i)) \| (m[0] \| \dots \| m[b]))$ (via oracle)

$\quad$ if t_guess $= t$ then

$\quad\quad \hat{m} = (m[0] \| \dots \| m[b] \| (t \| i))^{2} \| (m[0] \| \dots \| m[b])$

$\quad\quad \hat{t} = t \| i$

$\quad\quad$ return $(\hat{m}, \hat{t})$

$\mathrm{Exp}_{SE}^{\text{weak-ow-cca}}(A)$

$\quad k \xleftarrow{\$} Kg$

$\quad n^* \xleftarrow{\$} \mathcal{N}$

$\quad m^* \xleftarrow{\$} \mathcal{M}$

$\quad c^* \xleftarrow{\$} \mathrm{Enc}_k^{n^*}(m^*)$

$\quad \hat{m} \xleftarrow{\$} A^{D(\cdot,\cdot)}(n^*, c^*)$

$D(n,c)$ require $(n,c) \neq (n^*, c^*)$

$\quad m \leftarrow \mathrm{Dec}_k^{n}(c)$

$\quad$ return m

1) Show CBC Mode is not weak OW-CCA-secure

$\mathrm{Enc}_k^n(m)$	$\mathrm{Dec}_k^n(m)$
$c[0] \leftarrow n$	$c'[0] \leftarrow n$
for $i \in [1, \ldots, n]$	for $i \in [1, \ldots, n]$
$\quad X[i] \leftarrow m[i] \oplus c[i-1]$	$\quad X'[i] \leftarrow D_k(c'[i])$
$\quad c[i] \leftarrow E_k^n(X[i])$	$\quad m'[i] \leftarrow c'[i-1] \oplus X'[i]$
return $c[1] \Vert \ldots \Vert c[n]$	return $m'[1] \Vert \ldots \Vert m'[n]$

$\mathrm{Dec}_k^n(c[0] \Vert \ldots \Vert c[b] \Vert 0^L)[0:b] = D_k^n(c[0] \Vert \ldots \Vert c[b])$

$\cancel{\rightarrow c'[0] \leftarrow n}$

$\cancel{\rightarrow X'[1] \leftarrow D_k(c'[1]) = D_k(E_k(\ldots)) = c[1] =}$

$\cancel{\rightarrow X'[1] \leftarrow D_k(c'[1]) = D_k(c[1]) = D_k(E_k(X[1])) = X[1] = m[1] \oplus c[0] = m[1] \oplus n}$

$\cancel{\rightarrow m'[1] \leftarrow c'[0] \oplus X'[1] = n \oplus m[1] \oplus n = m[1]}$

$\cancel{\Downarrow}$

$\cancel{\rightarrow m'[i] \leftarrow m[i]}$

2) given $c[1] \| c[2]$ and n s.t. $c[1] \| c[2] = \mathrm{Enc}_K^*(m[1] \| m[2])$

find $m[1] \| m[2]$ with only querying 2 blocks

$A(n^*, c^*[1] \| c^*[2])$

$\cancel{\hat{m}[1] \| t \leftarrow D(n^*, c^*[1] \| 0^\ell)}$

$\cancel{t = 0^\ell \oplus Y[1] = 0^\ell \oplus E_k(X[1]) = \ldots E_k(n^* \| \langle 1 \rangle \ldots)}$

$\cancel{\_ \| u \leftarrow D(n^*, 0^\ell \| c^*[2])}$

$\cancel{u = c^*[2] \oplus Y[1] = c^*[2] \oplus E_k(X[1]) = c^*[2] \oplus E_k(n^* \| \langle 1 \rangle \ldots)}$

$= m[2]$

$\cancel{\hat{m}[2] \leftarrow t \oplus u}$

$\cancel{t \oplus u = E_k(n^* \| \langle 1 \rangle \ldots) \oplus}$

$\hat{m}[1] \| \_ \leftarrow D(n^*, c^*[1] \| 0^\ell)$

$\_ \| \hat{m}[2] \leftarrow D(n^*, 0^\ell \| c^*[2])$

3) a) $E\text{-}T\text{-}M\hat{}_{K_1, K_2}(m)$

$c \leftarrow \mathrm{Enc}_{K_2}(n, m)$

$t \leftarrow \mathrm{Tag}_{K_1}(n, c)$

return $c \| t$

$V\text{-}T\text{-}D\hat{}_{K_1, K_2}(c \| t)$

if $\mathrm{Vfy}_{K_1}(n, t)$

return $\mathrm{Dec}_{K_2}(n, c)$

else return $\perp$

b) (n^*, c^*) another valid (n', c')

If the underlying block cipher is vulnerable to length extension attacks then can use that. i.e. split c^* into c and t then perform length extension on c s.t. it will still tag to the same and then re-combine with the tag t.