CS 202 - Introduction to Applied Cryptography **Fall 2016**

HomeWork 4

November 9, 2016 *Liangjian Chen*

Problem 1 **Solution:**

OFB Assume $m_0 = 0^n$ and $m_1 = 1^n$. Change the first digit of c to obtain c' and decrypt the c'. And the decrypt answer would be either $10^n(b=0)$ or $01^n(b=1)$.

CBC Assume $m_0 = 0^n$ and $m_1 = 1^n$, block length is l. and change the last bit of c to obtain c' and decrypt the c'. Since in CBC mode, last digit only affect last block. So after discarding the last block, answer would be either $0^{n-l}(b=0)$ or $1^{n-l}(b=1)$.

Problem 2 **Solution:**

(a) None of three applied. Recall the last homework 1(a), PRG would create a detectable output pattern if it has a detectable input pattern. So $G([k|0])$ and $G([k|1])$ is not PRG anymore, so it is not Indistinguishable. Since not Indistinguishable, it is not CPA or CCA secure as well.

(b) it is Indistinguishable but not CPA-secure and not CCA-secure.

F(k,k) is same as PRG.So it works like OTP. But not CPA or CCA secure.

(c) it is Indistinguishable and CPA-secure but not CCA-secure.

Because, $G(F(r,k))$ is same as a PRF. So it work as construction 3.30 in text book. which is CPA-secure.

(d) it is Indistinguishable and CPA-secure but not CCA-secure.

Since G is a PRG, then we can see k_L and k_R is two independent keys.Thus v is same as construction 3.30 in text book and t is a random function's mapping for v which could not provide any more information. Thus this scheme works same as construction 3.30 which is CPA-secure.

Problem 3 **Solution:**

(a) Assume we have got a pair(m, t_1), then ask $t_1|x$ to obtain$(t_1|x, t_2)$. Then we now a valid new pair $(m|x, t_2)$.

(b) Assume we have got two triples (IV_1, m_1, t_1), (IV_2, m_2, t_2). Then we find all different bits between IV_1, IV_2. Then change the corresponding bits on m_1 to obtain $m3$. Now we get a new valid triple $(IV_2, m_3, t1)$. Because in CBC-MAC, input is the XOR of IV and first message block. If we change all bits different of m_1, then the input of first block is same (i.e. $IV_1 xor m_1 = IV_2 xor m_3$) and rest of block are same.

(c) Easily know $F_k(m_1) = t_1$, then we change $m_l = t_{l-1} \oplus m_1$ to get a new massage. and only final tag change which should be t_1 now. Thus we obtain a new pair$(m_1|m_2|..|m_{l-1}|(t_{l-1} \oplus m_1), t_1|t_2|..|t_{l-1}|t_1)$.

Problem 4 **Solution:**

if we have already get $a = M(k|x) = H(k|x|pad_x)$, then for any data y we feed $a|y$ then assume $b = H(a|y|pad_y) = H(k|x|pad_x|y|pad_y) = M(k, x|pad_x|y|pad_y)$. So without query the $x|pad_x|y|pad_y$, we get a new valid pair $(x|pad_x|y|pad_y, b)$.

Problem 5 **Solution:**

(a) No, if $|m|= n$ and $m = m'|0$ holds, then $H(m) = H(m')$. if we ignore the length then, two string would be same after padding.

(b) Yes, Assume $I_i = z_{i-1}||x_i$. First we can see that $H(m) = H(m')$ iff $|m|= |m'|$. Then we proof that $x_i = x'_i$. To proof that, first we notice that $I_{B+2} = I'_{B+2}$. otherwise a collision found in h. for any integer i, $I_x = I'_x$ holds for all $x \geq i$, then $I_{i-1} = I'_{i-1}$. Because if $I_{i-1} \neq I'_{i-1}$, we will capture an collision. Thus $\forall i, I_i = I'_i$ which indicate that $\forall i, x_i = x'_i$. i.e. a collision in H will lead to a collision in h, but h is a collision resistant function, so is the H.

(c) Yes, if $|m|= |m'|$, the proof will be same as (b). otherwise we will find a collision in last step($h^s(x_B||L) = h^s(x'_B||L')$ however $L \neq L'$.

(d) Yes, if $|m|= |m'|$, the proof will be same as (b). Th tricky part is $|m|\neq |m'|$. Let's assume $\ell = |m|$ and $\ell' = |m'|$ and $\ell > \ell'$. By follow the same idea on (b), we can find the only to way construct a collision H, without having collision on h, is that after $\ell - \ell'$ times iterator, the H outputs ℓ'. For example, $m = x_1|x_2|x_3|x_4$, $h^s(h^s(4||x_1)||x_2) = 2$, then $H(m) = H(x_3||x_4)$. However if we take expect value of how many times we need to try to find a collision, we can see it is exponential result(same with birthday paradox). i.e.

$$1 \cdot \frac{1}{2^n} + 2 \cdot \frac{2^n - 1}{2^n} \cdot \frac{2}{2^n} + 3 \cdot \frac{2^n - 1}{2^n} \cdot \frac{2^n - 2}{2^n} \cdot \frac{3}{2^n} + ... + 2^n \frac{(2^n - 1)!}{2^{(2^n-1)*2^n}} \cdot \frac{2^n}{2^n} = O(2^{n/2})$$