קריפטו מטלה 3

עוז לוי 305181158

שאלה 1 סעיף א'.

לפי הגדרת המשפחה, אורכו של הטאג אשר יוצר האלגו' שווה לעשרה ביטים עבור קלט כל כל מחרוזת בארוך n כלשהו.
לכן, כאשר n>10, אנו נווכח לכך כי בהכרח קיימות שני מחרוזות שונות באורך n אשר אם נשתמש בהן בתור קלט לאלגו' MAC אנו נקבל כתשובה טאג זהה.
רעיון: קיימות 2^n מחרוזות ו 2^{10} טאגים, לכן קיימות לפחות $2^n/2^{10}$ מחרוזות אשר אלגו' MAC יתן כתשובה את אותו הטאג.

הוכחה: נניח כי לכל טאג t מתוך T קיימות $0<x_i<2^n/2^{10}$ ($0<i<=2^{10}$)מחרוזות מתוך M אשר מקיימות
$MAC_k(m_1) = ... = MAC_k(m_x) = t$
עבור מפתח k אשר מופק באופן רנדומלי ע"י $Gen(1^n)$ מתוך K.
מכך קיימות $\sum_1^{2^{10}} Xi$ מחרוזות מתוך M אשר ניתן לקבל עבורן טאג מתוך T כפלט לאלגו MAC שלנו.
בנוסף $2^n > \sum_1^{2^{10}} Xi$, זאת סתירה להגדרת משפחת קודי אותנטיקציה.

מסקנה: מצאנו כי קיים טאג t אשר ניתן כפלט עבור לפחות שני מחרוזות שונות וההסתברות להפיק אותו ע"י אלגו' MAC היא $½^{10}$ וזאת אינה הסתברות זניחה – סתירה להגדרה מ.ז.ל.

שאלה 1 סעיף ב'.

נניח בשלילה כי המשפחה אינה מקיימת את ההגדרה הנ"ל אזי קיים תוקף A המשיג יתרון שאינו זניח.
A מצליח למצוא m_1,m_2 מתוך M ו t מתוך T כך ש $Verify_k(m_1,t) = Verify_k(m_2,t) = 1$
עבור מפתח k כלשהו אשר מופק באופן רנדומלי ע"י $Gen(1^n)$ מתוך K
בהסתברות שאינה זניחה ב n.

לפי הגדרת המשפחהMAC היא פונקציה רנדומלית חד ערכית וכיוונית ומתוך MxK אל T.
ע"י זאת נתאים לכל מחרוזת m מתוך M טאג יחיד t מתוך T בכדי לקיים את הגדרת existential unforgability, ז"א

For every $k = Gen(1^n)$ from K
And For every m_1,m_2 such that $m_1 != m_2$
$MAC_k(m_1) != MAC_k(m_2)$

בנוסף, היות כי MAC_k לקוחה מתוך משפחת פונק' אקראיות, העובדה כי A שתקף הצליח להפר את נכונות המערכת שלנו, אומרת כי
טענה א': או ש A הצליח להבחין ב MAC_k מתוך משפחת הפונ' האקראיות.
טענה ב': או ש A הצליח להפיק את אותו k שבו אנו השתמשנו.
שניהם יכולים לקרות בהסתברות זניחה 2^{-n}
אם טענה א' מתקיימת, אזי התוקף שלנו מצליח להבחין בהפונ' אקראית מתוך המשפחה, וזאת סתירה להגדרת משפחת הפונקציות האקראיות.
אם טענה ב' מתקיימת, אזי התוקף שלנו מחזיק בפתרון עבור בעיית ההבחנה בין פונ' אקראית לבין פסאודו-אקראית, שזו גם סתירה.

שאלה 2 סעיף א'.

Lets buils an attacker A that uses our MAC such that:

$M, M' = \{0,1\}^n$

All i from [1,n] , $m_i = \{0,1\}^n$

$K = Gen(1^n)$

$M = m_1 , m_2 , ... , m_l , m_{l-1}$

$M' = m_1 , m_2 , ... , m_{l-1} , m_l$

Sends $<M, MAC_k(M')>$

We can see that : $Ver_k (M,MAC_k(M')) = 1$ AND $M != M'$

Because m_1 XOR m_2 XOR ... XOR m_l XOR m_{l-1} = m_1 XOR m_2 XOR ... XOR m_{l-1} XOR m_l

Contradiction to the defenition

שאלה 2 סעיף ב'.

First, notice that our attacker can work polynomiclly, so he can find our specific k that we used.

And because it is neccerally that:

for every m,m' such that:

$|m| = |m'| = n$

for every $0<i<|m|-2$

$m_i = m'_i$

$m_{l-1} = m'_l$

$m_l = m'_{l-1}$

we can notice that:

$f_k(m_1),\ldots, f_k(m_l), f_k(m_{l-1}) = f_k(m'_1),\ldots, f_k(m'_{l-1}), f_k(m'_l)$

so same as the last paragraph its a contradiction.

שאלה 2 סעיף ג'.

בגלל שהיא אקראית, לא ניתן באמת להבחין.אי אפשר לדעת את k.

שאלה 2 סעיף ד'.