עבודה באבטחה - חלק ב- קריפטוגרפיה

3. א. $\Delta(a,b,c) = b,c,a$ נתון.

$\Delta(b,c,a) = c,a,b$

$\Delta(c,a,b) = a,b,c$

ולכן שמצאנו את הצפנה לא חזק כי:

$\Delta^3(a,b,c) = a,b,c$

ב. $\pi(x,y,z) = x',y',z'$ נתון.

1) $\pi(x,y,z) = x\oplus f(y,k_1),\ y\oplus f(z,k_2),\ z$

2) $\pi(x\oplus f(y,k_1), y\oplus f(z,k_2), z) = x\oplus f(y,k_1)\oplus f(y\oplus f(z,k_2),k_1),$

$y\oplus f(z,k_2)\oplus f(z,k_2),\ z =$

$= x\oplus f(y,k_1)\oplus f(y\oplus f(z,k_2),k_1),\ y,\ z$

3) $\pi(x\oplus f(y,k_1)\oplus f(y\oplus f(z,k_2),k_1), y, z) =$

$= x\oplus f(y,k_1)\oplus f(y\oplus f(z,k_2),k_1)\oplus f(y,k_1),\ y\oplus f(z,k_2),\ z =$

$= x\oplus f(y\oplus f(z,k_2),k_1),\ y\oplus f(z,k_2),\ z$

4) $\pi(x\oplus f(y\oplus f(z,k_2),k_1),\ y\oplus f(z,k_2),\ z) =$

$= x\oplus f(y\oplus f(z,k_2),k_1)\oplus f(y\oplus f(z,k_2),k_1),\ y\oplus f(z,k_2)\oplus f(z,k_2),\ z =$

$= x,y,z$

ומצאנו ש- $\pi^4(x,y,z) = x,y,z$.

ג) ידוע מסעיפים א' ו-ב' כי Δ^3 ו-π^4 הן פונקציות זהות ולכן אפשר לצמצם אותן בכל מקום בלי שינוי

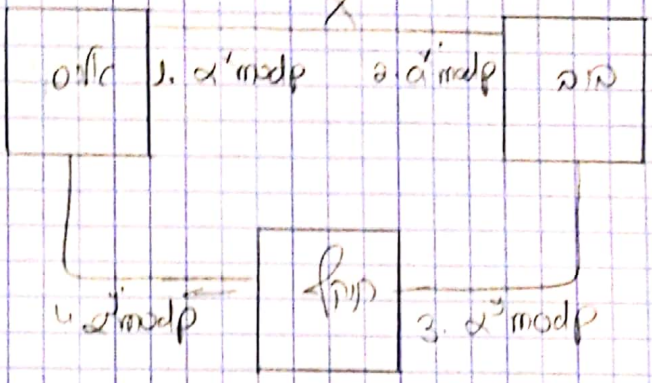
$\pi_3^{\,3}\,\Delta^2\,\pi_2^{\,3}\,\Delta^2\,\pi_1^{\,3}$

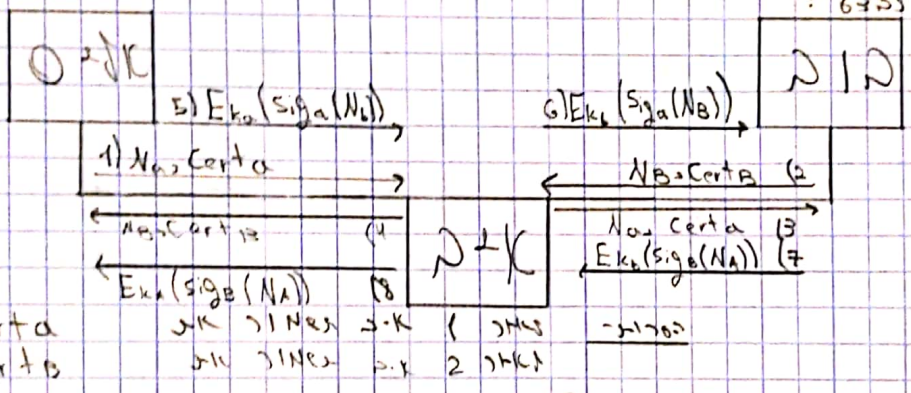
הוכחה: ה... נוכל

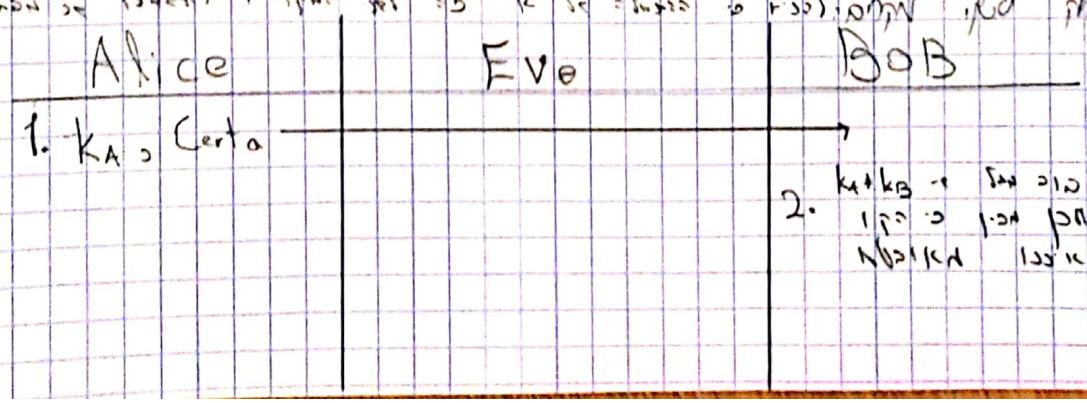
$\pi_3(\Delta(\pi_2(\Delta(\pi_1(m))))) \overset{\pi_3^3}{\Rightarrow} \pi_3^4(\Delta(\pi_2(\Delta(\pi_1(m))))) = \Delta(\pi_2(\Delta(\pi_1(m)))) \overset{\Delta^2}{\Rightarrow}$

$\Rightarrow \Delta^2(\Delta(\pi_2(\Delta(\pi_1(m))))) = \Delta^3(\pi_2(\Delta(\pi_1(m)))) = \pi_2(\Delta(\pi_1(m))) \overset{\pi_2^3}{\Rightarrow}$

$\pi_2^4(\Delta(\pi_1(m))) = \Delta(\pi_1(m)) \Rightarrow \Delta^3(\pi_1(m)) = \pi_1(m) \Rightarrow \pi_1^4(m) = \boxed{m}$







4) ג) מודל של...

Alice	Eve	Bob
1. k_a, $Cert_a$ →	2. k_B, $Cert_b$ →	3. מחליף את k_a ב-k_B
← 6. [illegible] k_a, k_b [illegible]	← 5. $E_{k_a}(Sig_b(k_b))$	← 4. $E_{k_B}(Sig_b(k_B))$

5) [illegible] כי [illegible] $Rand_1$ [illegible]
[illegible] את המפתח הפרטי [illegible]
[illegible] את ההצפנה [illegible]
המפתח הפרטי [illegible] $Rand_1$

ב) לא. השולח [illegible] יחד [illegible] מתקפה [illegible]. הפרוצדורה המוצגת חסין
שהמתקפה [illegible] ניתן [illegible] $RAND_2$ [illegible] אשר
[illegible] ההצפנה [illegible] $RAND_1$, [illegible] אשר [illegible]
[illegible] המפתח הבסיסי [illegible] את ההצפנה [illegible]
[illegible] מתקפה [illegible] פרוטוקול זה חסין.

6) א. נסמן M - plainText את ההודעה ו- C - cipherText (מוצפן).
אם מפתחות k_1, k_2 [illegible]. כמו כן [illegible] $k_3 = C'$
כך ש- C' [illegible] C [illegible]
$|k_3| = |C'|$ (אורך [illegible]).
[illegible] את k_3
[illegible] ש- k_1, k_2, k_3 [illegible]
נחשב: $m' = ShiftRow\{AES^*_{s}\{AES^*_{s}\{m\}_{k_1}\}_{k_2}\}$
ונקבל:

$$m' \oplus k_3 = C \Leftrightarrow m' \oplus C = k_3$$