בס"ד

26/12

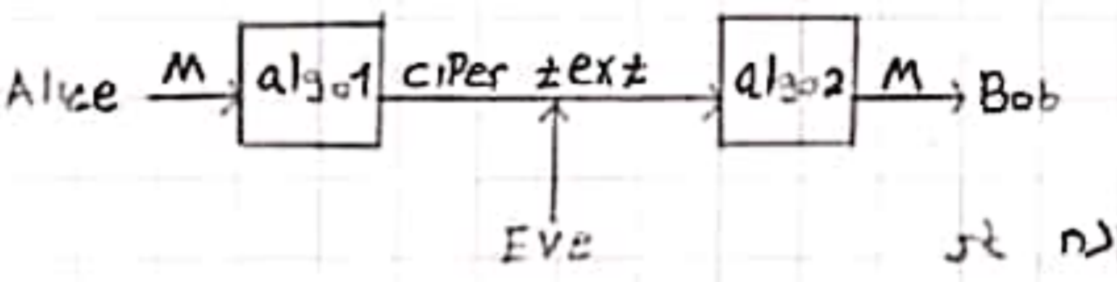
# אלגוריתם RSA

## א) הקדמה

אלגוריתם RSA מייצר הצפנה של טקסט. אנו נלמד על שני פעולות שניתן לממש אותם באמצעות RSA, פעולות אלו הם: הצפנת הודעות, וחתימה דיגיטלית.

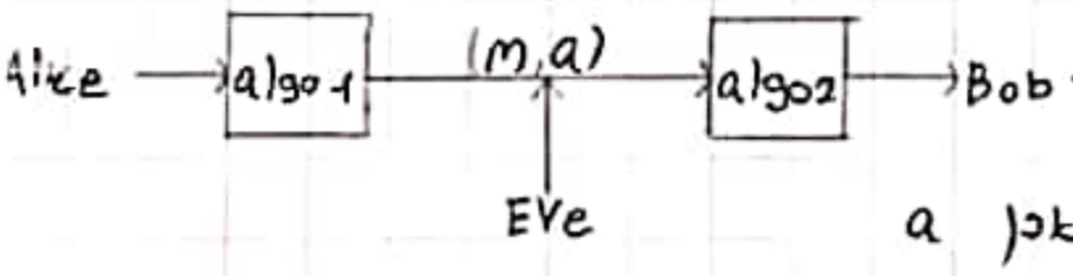
### הצפנת הודעות

להסביר פעולה זו נשתמש בדוגמא הבאה שתשמש אותנו לכל פרק זה. אליס רוצה לשלוח הודעה לבוב אך היא רוצה שרק בוב יוכל לקרוא אותה ולא שום אדם אחר. איב מנסה לצותת להודעה זו. לשם כך ישנו אלגוריתם שמצפין את ההודעה ושולח אותה לבוב מוצפנת, כך שאיב לא יכולה להבין. אצל בוב יש אלגוריתם שמפענח את ההצפנה להודעה המקורית.



### חתימה דיגיטלית

בפעולה זו אליס רוצה לשלוח הודעה לבוב ולא אכפת לה שאיב תקרא אותה, אך היא רוצה שלא יהיה ניתן לשנות את ההודעה ושבוב ידע שזו היא ההודעה שאכן נשלחה ממנה. לשם כך היא משתמשת באלגוריתם שיוצר חתימה דיגיטלית a, כך שההודעה נשלחת כך (m,a). אצל בוב יש אלגוריתם שמוודא שהחתימה הדיגיטלית היא אכן a ולא חתימה אחרת של איב. איב יכולה לשנות את m אך לא את a, ואז בוב ידע שההודעה לא מ



## ב) גישות בקריפטוגרפיה

יש שתי גישות מרכזיות בקריפטוגרפיה שעם כל אחת ניתן לממש את שני הפעולות שהזכרנו. גישות אלו הן: מפתח הצפנה פרט' ומפתח הצפנה ציבורי.

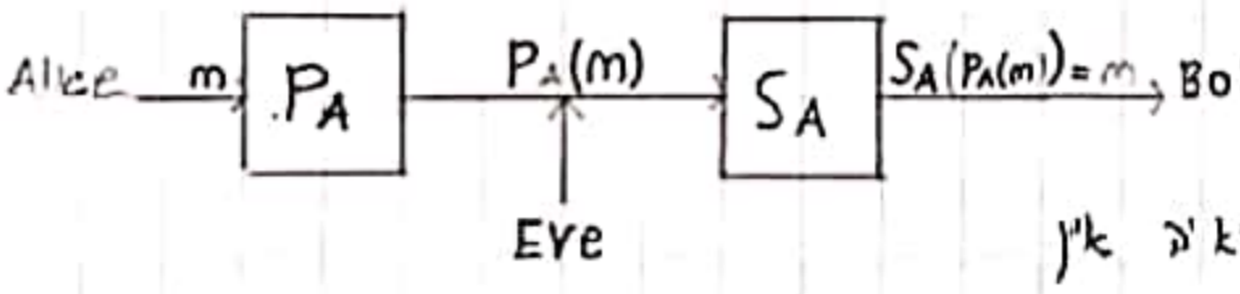
לאליס ובוב כל אחד יש שני מפתחות: מפתח ציבורי P ומפתח פרט' S, כך שבסך הכל ישנם ארבעה מפתחות: לאליס $P_A$ ו-$S_A$, ולבוב $P_B$ ו-$S_B$. מפתח פרט' P הוא אלגוריתם שמצפין טקסט, ומפתח ציבורי S הוא אלגוריתם שמפענח את הטקסט שהמפתח הפרט' הצפין. נסביר זאת בצורה מתמטית. נסמן את קבוצת כל האותיות ב-M. ארבעת המפתחות הם בעצם ארבעה פונקציות מהצורה $F: M\to M$ כלומר הם לוקחות אות מסויימת ומחזירות אות אחרת. הפונקציה $S_A$ הופכית לפונקציה $P_A$ כך שמתקיים: $P(S(m))=m=S(P(m))$, כלומר $P_A$ לוקחת את $m\in M$ ומשנה אותה, ו-$S_A$ מחזירה אות לאות המקורית. כמו כן $S_B$ הופכית ל-$P_B$

26/12

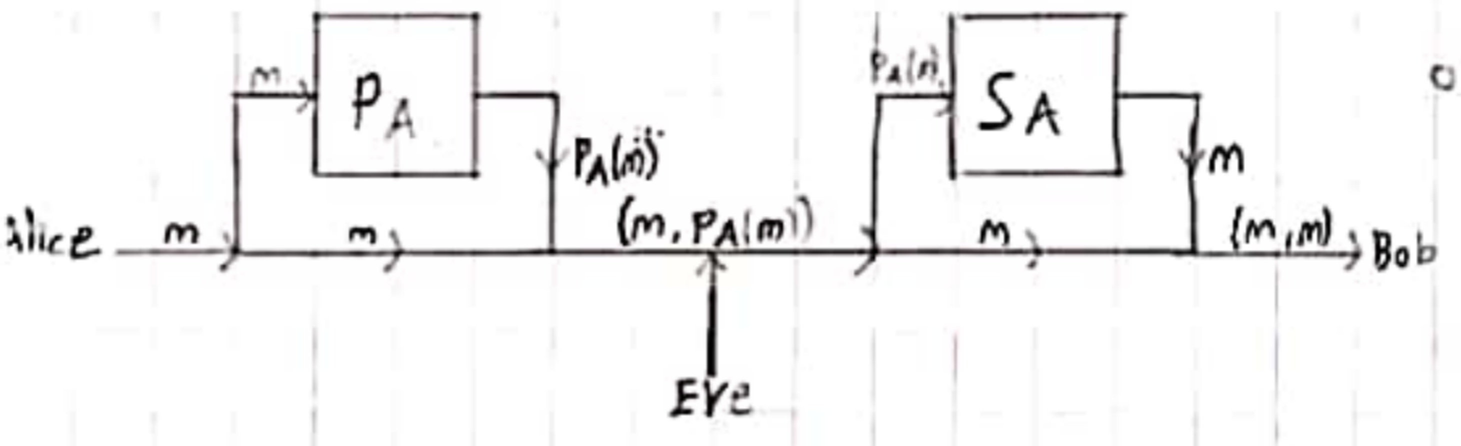
בס"ד

ההבדל שבין שתי הגישות בקריפטוגרפיה הוא שבמפתח הצפנה ציבורי ה-$P_A$ וה-$P_B$ של אליס ובוב גלוי לכולם ורק $S_A$ ו-$S_B$ נשאר בסודיות אצלם, ואילו במפתח הצפנה פרטי כל ארבעת המפתחות אינם גלויים לכולם. נסביר את מימוש הפעולות בכל אחת מהגישות:

## מפתח הצפנה פרטי (Private Key Encryption)

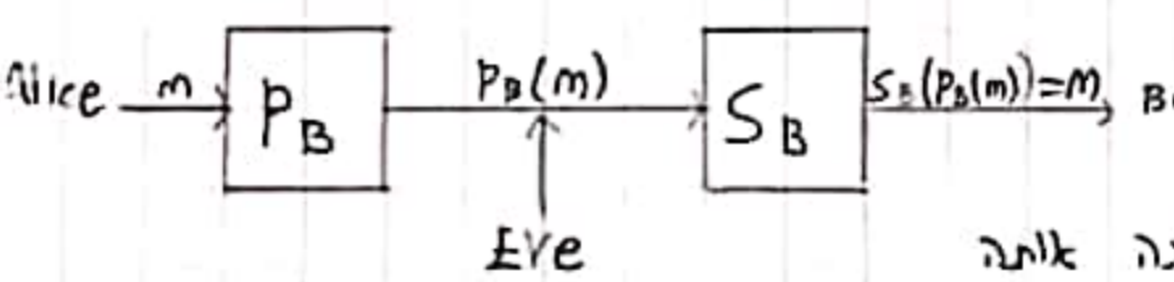


(1) הצפנת הודעות - לאליס יש את $P_A$ שמצפין טקסט ולבוב יש את $S_A$ שמפענח את הטקסט חזרה ל-$m$. לאיב אין את $S_A$, לכן אם תצותת היא תקבל $P_A(m)$ שאינה יכולה לפענח. במידה ובוב ואליס אינם נפגשים כך שאינה יכולה להביא לו את $S_A$ צריך גורם שלישי אמין (ממשלות, סוכנויות ביון וכו') שניתן לסמוך עליהם ולתת להם את $S_A$ שיעבירו לבוב. הקו מאובטח.

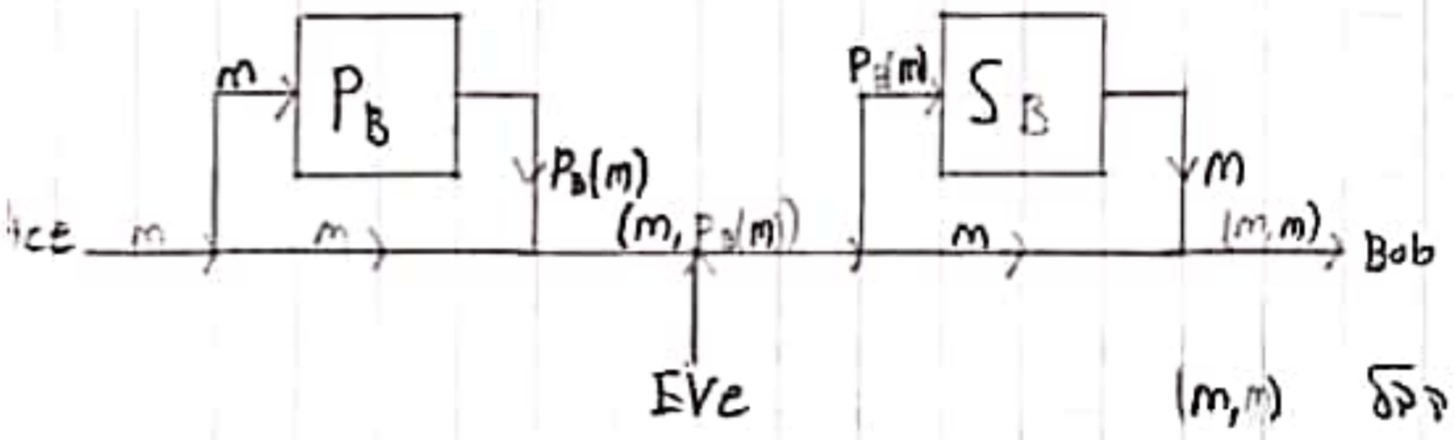


(2) חתימה דיגיטלית - בחתימה דיגיטלית שוב לאליס יש את $P_A$ שמצפין טקסט ולבוב יש את $S_A$ של אליס שמפענח טקסט חזרה ל-$m$. כאן אליס שולחת את $m$ עם ההצפנה שלו $P_A(m)$. בוב שמקבל $(m,P_A(m))$ מפענח את $P_A(m)$ באמצעות $S_A$, אם מקבל $(m,m)$ כלומר שיש תיאום ההודעה מאליס. איב יכולה לנסות לשנות את $m$ ל-$m'$ אך לא תצליח לשנות את $P_A(m)$ כך שישלח $(m', P_A(m))$. בוב בסוף יקבל $(m',m)$ ואז ידע שההודעה לא מאליס מפני ש-$m' \neq m$ כלומר אין תיאום בין ההודעות.

## מפתח הצפנה ציבורי (Public Key Encryption)



(1) הצפנת הודעות - כאן $P_A, P_B$ ידועים לכל. לאליס יש את $P_B$, לכן היא שולחת לבוב את $m$ אחרי שהצפינה אותה באמצעות $P_B$. איב אפילו שיש לה את $P_B$ ואת $P_B(m)$ אינה יכולה לפענח מפני שאין לה את $S_B$. בוב מפעיל את $S_B$ על $P_B(m)$ ומקבל את $m$. בשיטה זו לא צריך גורם שלישי אמין כמו במפתח הצפנה פרטי במידה שאליס ובוב לא נפגשים.



(2) חתימה דיגיטלית - שוב לאליס יש את $P_B$ ולבוב את $S_B$. אליס שולחת את $(m,P_B(m))$ ובוב מפענח את $P_B(m)$ באמצעות $S_A$. אם מקבל $(m,m)$ ההודעה מאליס. איב יכולה לשנות את $m$ ל-$m'$ אך לא תצליח לשנות את $P_B(m)$, ואז בוב יקבל $(m',m)$ וידע שההודעה לא מאליס כי אין תיאום.

## ג) כיצד עובד אלגוריתם RSA

לאחר שהבנו כיצד ממשים את שני הפעולות באמצעות שתי הגישות, נשאר ללמוד כיצד יוצרים את ארבעת הפונקציות: $P_A, S_A, P_B, S_B$. יצירת פונקציות אלו נעשות באמצעות אלגוריתם RSA נחלק את פעולת האלגוריתם לחמישה שלבים:

## אלגוריתם RSA

פלט: $P_A$ ו-$S_A$, כך שמתקיים: $P_A(S_A(m))=m=S_A(P_A(m))$.

(1) מוצא שני ראשוניים $p$ ו-$q$ גדולים מאוד! (באלגוריתמים 2 לומדים כיצד).

(2) קובע כי $n=p\cdot q$.

(3) מוצא מספר $e$ אי-זוגי כך ש-$(e,\varphi(n))=1$.

(4) קובע כי $d$ היא ההופכי מודולארי של $e$ מודולו $\varphi(n)$, כך שמתקיים: $e\cdot d\equiv 1\,(\varphi(n))$.

(5) האלגוריתם פולט: $P=\{e,n\}$, $S=\{d,n\}$.

האלגוריתם פולט זוגות סדורים, אם כן מהן הפונקציות? נסתכל על קבוצת כל האותיות $M$ כך שכל אות בה $m\in M$ מייצגת מחלקת שקילות ה-$n$. $\forall m\in\{[0]_n,[1]_n,\dots,[n-1]_n\}=[0,n-1]$.

כעת נוכל לבנות את הפונקציות לפי RSA ולפי האות מ-$M$ שנרצה בהם.

$$\begin{cases}P:[0,n-1]\longrightarrow[0,n-1]\\ P(m)=m^e\,(n)\end{cases}\qquad\begin{cases}S:[0,n-1]\longrightarrow[0,n-1]\\ S(m)=m^d\,(n)\end{cases}$$

הוכחה: נוכיח כי לכל $m\in[0,n-1]$ מתקיים: $P(S(m))=m=S(P(m))$ נעשה זאת בשני שלבים:

(1) נוכיח $P(S(m))=S(P(m))$. לפי הגדרת $P$ ו-$S$ נקבל: $P(S(m))=(S(m))^e\,(n)\Rightarrow(m^d)^e\equiv m^{de}\equiv(m^e)^d$

$\equiv(P(m))^d\,(n)=S(P(m))$ מ.ש.ל.

(2) יהי $m\in M$, יש להוכיח $P(S(m))=m$. מכיוון שהוכחנו לעיל כי $P(S(m))=m^{de}(n)$, יש להוכיח $m^{de}\equiv m\,(n)$ לפי משפט עזר 1 ממשפט שאריות סיני מכיוון ש-$n=p\cdot q$ מספיק להוכיח: (א) $m^{de}\equiv m\,(p)$ וגם (ב) $m^{de}\equiv m\,(q)$

(א) לפי הנחה $e\cdot d\equiv 1\,(\varphi(n))$. היות ו-$\varphi$ היא פונקציה כפלית וגם לכל ראשוני $p$ מתקיים: $\varphi(p)=p-1$ אזי $\varphi(n)=\varphi(p\cdot q)=\varphi(p)\cdot\varphi(q)=(p-1)(q-1)$. לכן $e\cdot d\equiv 1\,((p-1)(q-1))$, לפי הגדרת שקילות מתקיים: $(p-1)(q-1)\mid ed-1$. לכן קיים $k\in\mathbb{Z}$ כך ש-$ed=1+k(p-1)(q-1)$. נחזור להוכחת א'.

עבור $m\equiv 0\,(p)$ ניתן לראות שהטענה נכונה. לכן נניח $m\not\equiv 0\,(p)$. לפי המשוואה שהגענו אליה מק מתקיים: $m^{ed}\equiv m^{1+k(p-1)(q-1)}\equiv m\cdot(m^{(p-1)})^{k(q-1)}\,(p)$. היות והנחנו $m\not\equiv 0\,(p)$ אזי $p\nmid m$, לכן בהכרח $m$ ו-$p-1$ זרים. לכן נוכל להשתמש בפרמה הקטן עבור $m$ ו-$p-1$: $m^{p-1}\equiv 1\,(p)$. נציב זאת במשוואה ונקבל $m^{ed}=m\cdot 1^{k(q-1)}=m\cdot 1=m\,(p)$ מ.ש.ל. עבור ב' כמו א' רק מחליפים $p$ ב