|  |  |  |
| --- | --- | --- |
| **בי"ס להנדסת חשמל** | | |
| פרויקט מס' 21-1-1-2257  ***תכנית עבודה*** | | |
| שם הפרויקט: FPGA Implementation AES based Crypto Processor | | |
| מבצעים: | | |
|  | שם: אור רוב | ת.ז. 212199970 |
|  | שם: בנימין ריין | ת.ז. 211864194 |
|  | | |
|  |  |  |
| מקום ביצוע הפרויקט: אוניברסיטה  ***לשימוש המנחה:***  *הנני מאשר את תכנית העבודה המצורפת*  שם: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ חתימה:\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
|  | | |

# תקציר

תקציר הפרויקט הינו סיכום של מהות העבודה באורך **עמוד בודד** לכל היותר. חלק זה יכלול הסבר על נושא ותחום הפרויקט, היכן משתמשים בטכנולוגיות הקשורות לנושא הפרויקט וסקירה של אופן מימוש הפרויקט. יש להוסיף לפסקה זו **דיאגרמה של סביבת הפרויקט ו/או דיאגראמת בלוקים של הפרויקט**. תקציר ודיאגראמת בלוקים אמורים לאפשר לאדם שלא קורא את כל פרקי ספר הפרויקט לקבל תמונה כוללת של מהות העבודה.

בפרויקט זה נציג מימוש אשר משלב תת מעבד לצורך הצפנה (crypto- coprocessor ) במעבד גנרי. המעבד איתו נעבוד הוא- RISC V . נשתמש ב- AES-128 כ crypto- coprocessor  אשר ישולב במעבד. את מימוש ה AES נבצע על FPGA.

# מוטיבציה

בסעיף זה יש לתאר את המוטיבציה לביצוע הפרויקט (**חצי עמוד עד עמוד**). על פרק זה לכלול את **הסיבות ההנדסיות לקיומו של פרויקט זה**, מהי חשיבותו ותרומתו, וכל זאת בהשוואה למוצרים או טכנולוגיות קיימות. (יש לתאר בקווים כלליים לפחות 2 חלופות למימוש הפרויקט). **אין צורך** לכלול תיאור על המוטיבציה האישית לביצוע הפרויקט.

# תכולת עבודה

יש לתאר בפירוט מה יבוצע על ידי הסטודנטים במסגרת הפרויקט (**עד עמוד**). יש להתחיל מתיאור הרקע התיאורטי שעל הסטודנטים יהיה ללמוד וכיצד יבצעו זאת (יש לציין את רשימת הספרים/המקורות העיקריים שייסקרו לצורך הפרויקט). לאחר מכן יש לכלול תיאור מפורט עד כמה שניתן של **דרישות המערכת והשיטות והשלבים לביצוע ומימוש הפרויקט**. בחלק זה יש לכלול, ע"פ הרלוונטיות לפרויקט, את התשתית המדעית/מתמטית/הנדסית/ אלגוריתמית שעומדת בבסיס הפרויקט. יש לציין **באילו כלים שפות ורכיבים הסטודנטים ישתמשו למימוש כל שלב בפרויקט**: לדוגמא פלטפורמת PC, Android ,ARDUINO MATLAB, JAVA וכדומה.

בפרויקט הסטודנטים ילמדו לעומק את סטנדרט ההצפנה AES, ויגיעו לכדי מימוש חומרתי שלו – בלוק הצפנה ופיענוח.

כמו כן, הסטודנטים ילמדו ויחקרו את ארכיטקטורת המעבד (), ולאחר מכן יבצעו אינטגרציה של בלוק ה-AES לצנרת (pipeline) המעבד.

חלק ה- design של הפרויקט יבוצע בשפת Verilog על כרטיס FPGA של xlinx. בדיקות התקינות יבוצעו באמצעות סימולציות והרצות על הכרטיס. (ייתכן כי חלק מהפיתוח/בדיקות יתבצע בשפת PYTHON).

# תוצרי הפרויקט

יש לתאר מה יהיו תוצרי הפרויקט (**חצי עמוד עד עמוד**) : יש לתאר ולרשום את תכנם של **התוצרים שיושגו עד להגשת דו"ח המעקב ובסוף הפרויקט (תוצר אינו יכול להיות תיאורטי בלבד ועליו להכיל לפחות תוצאות סימולציה)**. ברשימת התוצרים צריך שתהיה בניית דגם/אב טיפוס או מודל מוקטן. אם אין אפשרות אז לפחות סימולציה פונקציונאלית תוך הנמקה. יש לפרט את הפונקציונליות שהתוצר ייצג בהתייחס לדרישות המערכת. בדיקת דו"ח המעקב ובחינת הפרויקט הסופית יתבססו על מילויה של רשימת תוצרים זו. **יש לפרט (עד חצי עמוד) מהו התוצר הסופי אותו יציג הסטודנט בבחינת הפרויקט**. יש לפרט נושאים לבדיקה ושיטות עקרוניות לבדיקת תוצרי הפרויקט, וכן תיאור של סביבת הבדיקות.

# לוח זמנים

בסעיף זה יש צורך לתאר את רשימת אבני הדרך של הפרויקט, עם תיאור מילולי קצר (2-3 שורות) של כל אבן דרך ותאריך יעד. יש לכלול בין 8-12 אבני דרך, בתוכן:

* תאריך יעד להגשת דו"ח מעקב
* תאריך יעד להגשת הפוסטר
* תאריך יעד לסיום הפרויקט

|  |  |  |  |
| --- | --- | --- | --- |
| אבן דרך | פירוט (2-3 שורות) | תאריך יעד לביצוע | הערות |
| 1. לימוד ומחקר החומר התיאורטי המתקשר לפרוייקט | למידה של החומר הפרקטי: שפת תיאור החומרה – ורילוג.  למידה של החומר הפרקטי:  אלגוריתם ההצפנה מבנה המעבד | 14.11.2021 |  |
| 2) צריבת המעבד הרגיל לFPGA ובדיקת תקינותו הכללית |  | 21.11.2021 | אבן דרך זאת תתבצע במקביל לאבן דרך מס' 1. |
| 3) תכנון אכטיקטורת מודל ההצפנה. | בניית דיאגרת בלוקים ותכנון כללי ברמת המקרו של מערכת ההצפנה | 19.12.2021 |  |
|  |  |  |  |
| 4) תכנון מיקרו אכטיקטורה למודל ההצפנה | תיאור מלא של כל המודלים המרכיבים את האכטיקטורה ותיאור הקשרים בין המודלים ברמת המיקרו של מערכת ההצפנה. | 7.01.2022 |  |
| 5) הגשת מצגת האמצע |  | 9.01.2022 |  |
| 6) דיזיין | ביצוע הקידוד של המיקרו אכטקטורה + דיבוג וורפיקציה | 8.05.2022 | יציאה לתקופת מבחנים עד ה 18.03.2022 |
| הגשת הפוסטר |  | 1.06.2022 |  |
| סיום הפרויקט |  | 7.06.2022 |  |