המרכז
האקדמי
לב

החוג להנדסת חשמל ואלקטרוניקה

Department of Electrical and Electronics Engineering

אלגוריתמים בקריפטוגרפיה ומימוש ב-Verilog

130330

Lecturer – מרצה

אורי שטרו

Uri Stroh

הקורס: סקירה כללית

- קורס זה (130330) עוסק במימוש בחומרה של אלגוריתמים מתורת ההצפנה (קריפטוגרפיה\קריפטולוגיה)
- המימוש בחומרה מתבצע במסגרת הקורס תוך שימוש **בשפת Verilog**
- הקורס משלב הרצאות תאורטיות, מעבדות, תרגילים ולימוד עצמי
- הקורס כולל 4 שעות שבועיות כל יום א'. שעות אלו מחולקות להרצאה תאורטית ולמעבדות\תרגול **לפי שיקול דעתו הבלעדי של המרצה**

מטרות הקורס

בסיום הקורס יוכל הסטודנט

- **לתכנן** מעגל ספרתי תוך שימוש בשפת Verilog
- **לכתוב** מערך בדיקה (Test Bench) **תוך שימוש בשפת** Verilog
- **לתאר ולהסביר** מהי תורת ההצפנה
- **לתכנן בחומרה** מנגנונים עיקריים של אלגוריתמים קריפטוגרפיים

עקרון הלימוד של שפת Verilog...

כמה ציטוטים

- **למדתם VHDL?** "אתם יודעים Verilog, רק אתם לא יודעים שאתם יודעים.." (ציטוט מחבר טוב, קולגה לעבודה)
- **Verilog?** "כשהגעתי לעבודה חדשה למדתי Verilog תוך שעה וחצי..." (סטודנט בוגר המכון, עובד בחברה ביטחונית)
- **פתגם סיני עתיק:** "תנו לאדם דג, והוא יהיה שבע לאותו יום. למדו אותו לדוג והוא יהיה שבע כל חייו"

שיטת הלימוד בקורס מתבססת על הידע הקיים של הסטודנט בשפת VHDL במטרה להביא את הסטודנט ליכולת עבודה בשפת Verilog, תוך מימוש אלגוריתמים קריפטוגרפיים.

קיימות דרכים אחרות, לגיטימיות, ללימוד Verilog...

דרישות מקדימות

- הקורס מיועד לסטודנטים שעברו בהצלחה את **שני הקורסים בתכנון ספרתי (תכנון ספרתי מתקדם, ומעבדה בתכנון ספרתי ממוחשב)**
- ומכאן שהתלמיד כבר עבר בהצלחה:
  - ✓ **קורס לוגיקה ומערכות ספרתיות**
  - ✓ **קורס אלקטרוניקה כללית**
  - ✓ **קורס בשפת תוכנה** כלשהי
  - ✓ ולתלמיד **שליטה מוכחת באנגלית** (באמצעות קורס מתאים או פטור)

- **מדובר על קורס חדש יחסית**
- **הקורס מכיל מרכיבים משני תחומים שונים: קריפטוגרפיה ו-Verilog (מדובר במסגרת הכוללת באופן פרקטי שני קורסים)**
- **קורסים אלו (קריפטוגרפיה ו-Verilog) ניתנו לסטודנטים במסגרת פרויקטי גמר מספר שנים לפני שנפתחו לכלל הסטודנטים במחלקה כקורסי בחירה.**
- **במהלך השנים נעשו בחוג להנדסת חשמל ואלקטרוניקה פרויקטים רבים הכוללים שימוש בשפת Verilog ופרויקטים רבים במימוש בחומרה של אלגוריתמים בקריפטוגרפיה.**

שיטות הלימוד

- הקורס מבוסס על מגוון טכניקות הוראה
  - הרצאות בכתה
  - הדגמות על כלי תכנון ומחשבים
  - מעבדות (**תכנון** לומדים על ידי **תכנון**)
  - תרגילי בית
  - דיונים
  - לימוד עצמי
  - עבודת צוות
  - עבודה אישית
- לא כל הרצאה מבוססת על שקפים – אנא הכינו מראש דפים וכלי כתיבה

מבנה הציון

- 20% **תרגילים\מעבדות ("מטלות")**
- 10% **בוחן**
  1. תאריך מתוכנן לבוחן: ט"ז אייר תשפ"ו – 3/5/2026
  2. מרכיב ציון זה כולל בוחן, או מטלה מיוחדת בעלת היקף רחב לפי שיקול דעת של המרצה
  3. נוכחות במפגשי הקורס תזכה את הסטודנט בבונוס, בתוך מרכיב ציון זה
- 70% **מבחן סופי**

חלק ממטלות הקורס הן משימות קבוצתיות, באותן משימות תידרש נוכחות חובה לצורך ביצוען בכתה במסגרת קבוצתית (הודעה על אותן משימות תינתן מראש). משקל המטלות הקבוצתיות הוא מחצית ממשקל התרגילים.

מה צריך שיהיה לסטודנט כדי ללמוד בקורס

לפעמים צריך לרשום במפורש את המובן מאליו...

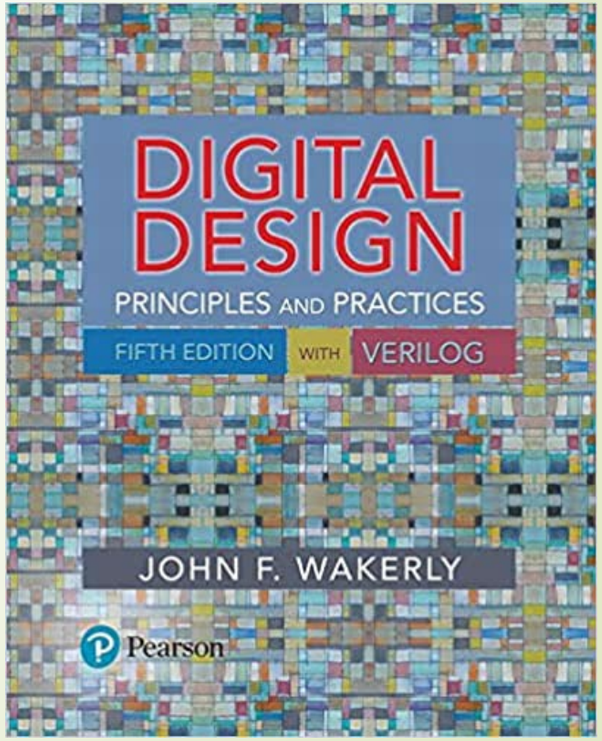
- גישה ל-Moodle
- חשבון מייל ב-g.jct.ac.il (נדרש כדי לצפות בהקלטות שיעורים)
- חיבור אינטרנט בפס רחב (כדי לצפות בשיעורי Zoom, בהקלטות שיעורים וכדי לגשת לשרת בו מותקנים כלי תוכנה רלוונטיים)
- מחשב (כדי לגשת ל-Moodle, ל-Zoom, להקלטות, לכלי התכנון)
- כלי כתיבה... כדי לסכם את השיעור
- **זמן...** כדי להשתתף בהרצאות
- **זמן...** כדי לחזור על חומר הלימוד לקראת כל שיעור
- **זמן...** כדי לבצע את המטלות ולהגיש אותם

ספרות וחומר עזר בנושאי תורת ההצפנה

- חומר שיחולק במסגרת הקורס

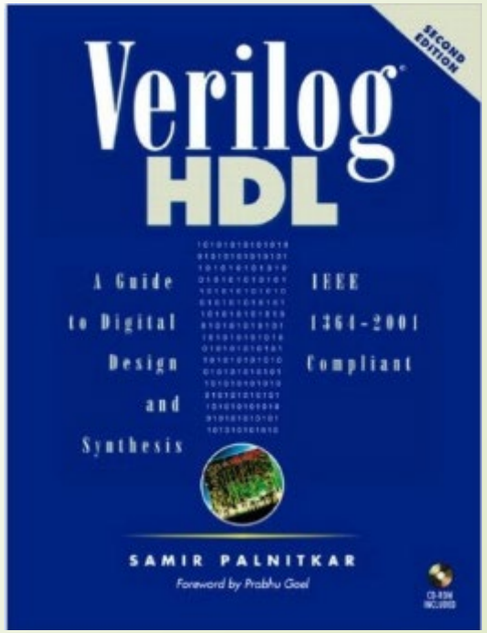
ספרות וחומר עזר בנושאי Verilog

- Digital Design: Principles and Practices (5th Edition)
- Author: John F. Wakerly
- Publisher: Pearson; 5th edition (July 24, 2018)
- ISBN-10: 013446009X
- ISBN-13: 978-0134460093



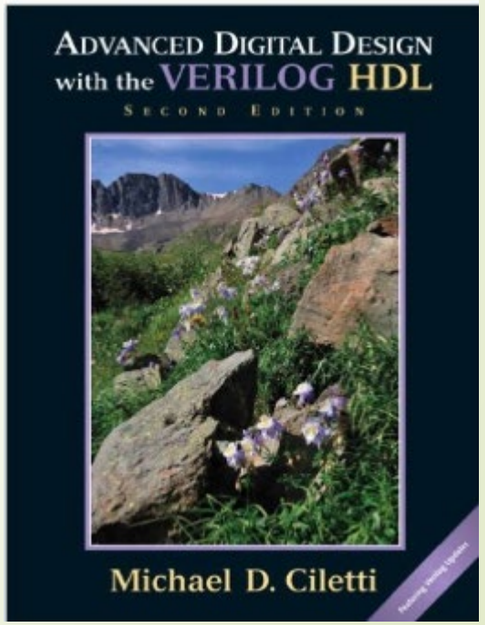
ספר מומלץ בנושא Verilog

- Verilog HDL (2nd Edition)
- Author: Samir Palnitkar
- Publisher: Prentice Hall; 2nd edition (July 2003)
- ISBN-10: 0132599708
- ISBN-13: 978-0132599702



ספר מומלץ בנושא Verilog

- Advanced Digital Design with the Verilog HDL (2nd Edition)
- Author: Michael D. Cileti
- Publisher: Pearson; 2nd edition (January 2010)
- ISBN-10: 0136019285
- ISBN-13: 978-0136019282



כמו בשנה שעברה

- דרוש איש קשר בין הסטודנטים למרצה

<u>תיאור התפקיד</u>

העברה מרוכזת של הודעות וחומר לימוד בין המרצה לסטודנטים

פניות אל המרצה

באפשרותכם לפנות אל המרצה בכל אחת מהדרכים הבאות:

- פניה בשעות קבלת תלמידים לשאלות\תשובות (בימי א' לאחר ההרצאה, בין 20:55 ל- 21:40)
- משלוח דואר אלקטרוני לכתובת stroh@jct.ac.il

  נא לרשום את שם הקורס במפורש בכותרת המייל (המרצה מעביר עוד קורסים...)
- פניה באמצעות איש הקשר

לֹא הַבַּיְשָׁן לָמֵד

אבות ב ,ה

אל תוותרו על הבנה של חומר הלימוד

- **אל תהססו לשאול שאלות** אם חומר הלימוד או הנושא אינו ברור לכם
- לפעמים, המרצה אינו נותן לשאול שאלה מייד, כי הוא באמצע הסבר או מהלך, שרק בסופו ניתן יהיה לשאול (ייתכן שהמשך ההסבר של המרצה ממילא יענה על השאלה). **תוכלו לשאול את השאלה עם סיום ההסבר**, כאשר המרצה ייתן זמן לשאלות.
- בגלל גודל הקבוצה, מספר השאלות שניתן לשאול במהלך הזמן המוקצב בשיעור מוגבל. **עדיין ניתן לפנות אל המרצה** לאחר ההרצאה (ראה בהסבר על "פניות אל המרצה")
- קרה ולא שאלת את המרצה (מאיזו סיבה שהיא), אנא השתדל לא לשאול את השכן... הרעש וההתלחשות בשאלה עלולים להפריע לשכן, לכל הכתה ואולי גם למרצה (**המרצה ממילא ישמח לענות אחר כך**)

וכמה דברים שחבל שצריך להזכיר אותם

(בפרט, לציבור של מהנדסים לעתיד, שהם אנשי תורה ומצוות)

אבל למרבה הצער, הסתבר שבשנים קודמות הם לא היו מובנים מאליהם...

- יש להגיע להרצאות בזמן
- יש לשמור על שקט בזמן ההרצאה (במיוחד, כאשר המרצה מבקש שמירה על השקט, הנדרשת לצורך הסבר הנושא הלימודי)
- "דעלך סני לחברך לא תעביד" - כאשר המרצה עונה לשאלה של סטודנט, המרצה מצפה שכל הכתה יהיו בשקט ויקשיבו לתשובה (ולפחות יכבדו את החבר שלהם, המקבל תשובה לשאלתו)
- העתקת תרגיל והגשת התרגיל המועתק - היא הונאה
- המרצה אינו שוטר ואינו גננת...

כמה דברים שעורכי הדין שלנו רוצים שתדעו...

כלי התכנון

- המרכז האקדמי לב חתום על הסכמים אקדמיים עם יצרניות מובילות של כלי תכנון לוגי, כגון:
  - **Mentor Graphics (כיום Siemens-EDA)**
  - **Synopsys**
  - **Xilinx-AMD**
- במסגרת הסכמים אלו מותקנים על מחשבי בית-הספר הגבוה לטכנולוגיה כלי תכנון של חברות אלו אלו בגירסה מלאה.
- לדוגמא, שמות של כמה מכלי התכנון שבהם תעשו שימוש במהלך הקורס (וזאת, מבלי לגרוע מהרשימה שמות של מוצרים אחרים הקיימים בבית-הספר במסגרת ההסכמים):
  - **סימולטור לוגי ModelSim/QuestaSin - VHDL/Verilog**
  - **כלי לסינטזה לוגית Precision**
  - **Vivado – כלי לתכנון רכיבי FPGA של חברת Xilinx-AMD**
- כלים אלו נועדו למטרות לימודיות בלבד. חל איסור מוחלט להשתמש בכלים אלו המותקנים במרכז האקדמי לב למטרה מסחרית כלשהי.

שימו לב: כלים מסויימים ניתנים על ידי יצרניות הכלים באופן לגיטימי, בגירסה חינמית או גירסת סטודנט. המרצה ממליץ לנצל הזדמנות לימודית זו ולהתקין את אותם כלים מותרים ולגיטימיים על המחשב האישי, בהתאם לתנאים המוגדרים על ידי יצרני הכלים. פרטים בהמשך הקורס...

חומר הקורס

- חומר הקורס מיועד לשימוש פנימי במחלקת אלקטרוניקה. חל איסור להעביר את חומר הקורס או חלקו בכל צורה שהיא מודפסת או אלקטרונית לאנשים שאינם רשומים לקורס.

“

יְהִי רָצוֹן מִלְּפָנֶיךָ ה׳ אֱ-לֹקֵינוּ וֵא-לֹקֵי אֲבוֹתֵינוּ ,שֶׁתּוֹלִיכֵנוּ לְשָׁלוֹם וְתַצְעִידֵנוּ לְשָׁלוֹם וְתַדְרִיכֵנוּ לְשָׁלוֹם, וְתִסְמְכֵנוּ לְשָׁלוֹם, וְתַגִּיעֵנוּ לִמְחוֹז חֶפְצֵנוּ לְחַיִּים וּלְשִׂמְחָה וּלְשָׁלוֹם.

”