**מבוא לתקשורת - איך תקשורת פועלת?**

כאשר נשלח מייל מנקודת קצה אחת לשנייה הוא עובר בכמה תחנות- router ,switch .   
הראוטר יודע לאן לנווט חבילה לפי אלגוריתמי ניתוב שחישבו מראש. לאו דווקא מהדרך הקצרה ביותר, אלא מהדרך הפנויה ביותר.  
אלגוריתמי ניתוב:

DVR- distance vector routing (local- מכיר רק את השכנים שלו)

LSR- link state routing (global-מראש לומד את המסלול ולא ישתנה בהתאם לדרך)

Subnet mask -

IP מכיל 4 שמיניות של BIT

יש רשת ענקית, כל מחשב מקבל IP. איך יודעים כמה כתובות לתת למחשבים? צריך לדעת את כמות המחשבים שצריך לתחזק. צריך לחלק את הרשת לניתוב החבילות החוצה\פנימה(לראוטרים), וחלק למחשבים.

IP \_ \_ \_ \_ \_ \_ \_ \_\*\_ \_ \_ \_ \_ \_ \_ \_\*\_ \_ \_ \_ \_ \_ \_ \_\*\_ \_ \_ \_ \_ \_ \_ \_

בדר"כ השמיניה האחרונה תהיה המקום של מספר המחשב. כמה שיותר מחשבים יש, ככה יותר שמיניות הם יתפסו.

**+** בין client לserver יש RTT – round trip time , זה הזמן תגובה בין הבקשה לתגובה בין שני מחשבים.

כל מה שמחובר לאינטרנט - host

נקודת גישה שממנה מקבלים אינטרנט - access point

חיבור בין הhost וrouters – link

Router- מטרתו לנתב חבילה ברשת

Switch- מטרתו לקדם חבילה ברשת

**+**Switch מקבל חבילה מ routerולוקח החלטה מה יעיל יותר ואיך לקדם את החבילה בצורה המהירה בדרך הפנויה ביותר.

Protocol- אוסף כללים (קונפיגורציות) שלפיהן פועלים ראוטרים ומחשבים

לרשת יש פורמט ידוע וסדר הגעת הנתונים ופעולות שעושים. בין מחשב לשרת צריך לבקש אישור להתחבר, לקבל אישור, לבקש קובץ ולשלוח קובץ

**שני סוגי העברת נתונים-**

1. אמין – לא יכול לאבד שום חבילה באמצע, איך שנשלח ככה התקבל (ואם נפלה חבילה בדרך הראוטר יודע להודיע ולבקש שישלחו את מה שאבד) TCP
2. לא אמין- דברים יכולים להעלם בדרך (למשל שיחה בסקייפ, סרט וידאו. כשאר הקול מקוטע, תמונה נתקעת) UDP

Pixel= 8 bits

Red Green Blue

**שני מודלים שעובדים איתם ברשת-**

1. Client\server model – צד לקוח\שרת- חייב להתחבר לשרת כדי להוריד מידע (יוטיוב, ג'ימייל)
2. Peer to Peer- שרת לא מעורב (טורנט)

**שני מודלים איך עובד אינטרנט-**

1. Circuit switching- יוצרים מעגל ובתוכו שולחים נתונים

כל משתמש במאגר מקבל משהו משלו : תדר [FDM- frequency division multiplexing](http://scholar.google.co.il/scholar?q=fdm+frequency+division+multiplexing&hl=en&as_sdt=0&as_vis=1&oi=scholart)))

או זמן (time division multiplexing TDM-)

1. Packet switchingשליחת חבילות ללא מעגל-

אינטרנט מודרני , כמו כאשר שולחים מייל והוא מתחלק לחבילות

**7 שכבות של תקשורת-**

**5 שכבות תקשורת ועוד 2 נוספות**

1. Application- שכבת אפליקציה
2. Presentation-שכבת הייצוג
3. Session- שכבת השיחה
4. Transport- שכבת התעבורה
5. Network- שכבת הרשת
6. Data Link- שכבת הערוץ
7. Physical- שכבה פיזית

בפועל יש מודל 7 שכבות, ויש מודל של 5 שכבות שפשוט בשכבה הראשונה נכנסות גם שתי השכבות של "ייצוג" ושיחה"

מתכנת אחראי רק לשתי השכבות "אפליקציה" ו"תעבורה". בניהן יש שתי שכבות "ייצוג" ו"שיחה".

רמה ראשונה (1)משתמש מפעיל תוכנה (מקיש כתובת בדפדפן, HTTP-קובץ), רמה שנייה(4) מתכנת צריך להחליט איך האתר עובד ואיך הוא יעבור, בשיטה האמינה או בשיטה הלא אמינה.

congestion control - עומס בתנועה (עומס בהעברת הנתונים עצמם, ז"א ככל שיש עומס יותר גדול סיכוי סביר שיותר חבילות ייפלו בדרך)

flow control- עומס אצל המקבל (מקבל יותר מידי חבילות שלא יכול להתמודד איתם, ז"א אם המקבל מקבל בו זמנית אימייל, שיחת סקייפ, ועוד חבילות)

**שני מודלים להעברת הנתונים:**

End to end- המסר יוצא ומגיע שלם לא משנה איך. (web, email)

Point to point- המסר מתחלק לחבילות ועובר בנקודות מסוימות switch, rauter. חבילות מסויימות יכולות ללכת לאיבוד בדרך. בשיטה זו יש כתובת, ניתוב (מציאת מסלול הכי קצר), וcongestion control.

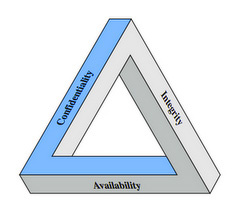
כאשר רוצים לתקוף צריך לדעת לחשב את שני המושגים הנ"ל, כדי לדעת מתי הזמן המתאים לפעול כדי לא ליפול בעצמינו בעומס.

**אבטחת מחשב**

**אבטחת המחשב (computer security) –** שם כללי עבור אוסף הכלים שמטרתם להגן על הנתונים וכדי לסכל האקרים.  
\* ההגנה שמוענקת למערכת מידע אוטומטיות בכדי להשיג את היעדים הרלוונטיים של שמירה על השלמות, זמינות, ושמירת סודיות (=שלושת הדרישות לאבטחה) של משאבי מערכת מידע. (כולל חומרה, תוכנה, קושחה, מידע/נתונים, ותקשורת).

**אבטחת הרשת (network security)–** אוסף כלים שנועדו להגן על נתונים במהלך השידור שלהם. / אמצעים להרתיע, למנוע, לגלות, הפרות אבטחה נכונות הכרוכות בכך - העברת מידע.

**דרישות האבטחה:**

* **שלמות** (integrity). הגנה מפני שינוי זדוני של המידע או השמדתו, כולל הבטחת [אי התכחשות](https://he.wikipedia.org/w/index.php?title=%D7%90%D7%99_%D7%94%D7%AA%D7%9B%D7%97%D7%A9%D7%95%D7%AA&action=edit&redlink=1) ו[אימות זהויות](https://he.wikipedia.org/wiki/%D7%90%D7%99%D7%9E%D7%95%D7%AA_%D7%96%D7%94%D7%95%D7%99%D7%95%D7%AA) בעלי המידע.   
  הבטחת שלמות הנתונים:
  + גיבוי
  + Checksums :קוד לזיהוי שגיאות
* **סודיות**(confidentiality)   
  הימנעות גילוי בלתי מורשה של מידע. סודיות כרוכה בהגנה על נתונים, מתן גישה למי מותר לראות את זה תוך הגבלת גישה או חשיפת מידע לאחרים.

**Data  
and  
Services**

הבטחת סודיות:

* + הצפנה : העברת מידע באמצעות הצפנתו ופיענוחו.
  + בקרת גישה: הכללים והמדיניות המגבילים גישה למידע סודי על ידי זהות, כגון שם אדם או מס' סידורי במחשב, או על ידי תפקיד שיש לאדם, כגון מנהל או מומחה לאבטחת מחשבים.
  + אישור: הפעולה שקובעת אם לאדם מותרת גישה למשאבים, בהתבסס על מדיניות בקרת גישה.
  + אימות: הפעולה שקובעת את זהות האדם, עפ"י טביעת אצבע, ת.ז, פנים, כל דבר שייחודי לאדם.
  + חומרתי חישובי
* **זמינות** (availability). שמירה על זמינות ויעילות הגישה אל המידע בכל זמן נתון. מבטיח כי מערכות עובדות מידית והשירות לא יישלל למשתמשים מורשים. (התקפה על זמינות dos ddos)

הבטחת זמינות:

* + **פיזית:**

מתבצעת ע"י חומרה נוספת כגון מחשב , שרת וכו'.

* + **חישובית:**

מחשבים והתקני אחסון המשמשים כגיבוי למקרה וישנו כשל במערכת.

**מודל הOSI**

מתמקד להתקפות אבטחה, מנגנוני ושירותים.

אבטחה התקפה: כל פעולה שכוללת את אבטחת המידע

בבעלות ארגון.

מנגנון האבטחה: תהליך (או התקן שילוב כזה

תהליך) המיועדת לזהות, למנוע או להתאושש אבטחה

התקפה.

Securityשירות: שירות עיבוד או תקשורת, אשר משפר את

האבטחה של מערכת עיבוד נתונים והעברות מידע

של ארגון.

**טרמינולוגיה**

**נכס**- דבר שנרצה להגן עליו:

* חומרה
* תוכנה
* נתונים

**חולשות-** מה שמחפשים בדר"כ כדי לתקוף (חולשה במערכת שניתן להכניס לה קוד זדוני ע"מ לגרום לה נזק):

* שרת קבצים שלא מאמת את המשתמשים , למשל גוגל דרייב , אם לא מאמת את המשתמש ועדיין אפשר להכנס.

**איומים-** אובדן או נזק שיכול לגרום לנפילת מערכת:

כל הקבצים יכולים להיחשף לציבור

4 קטגוריות של איומים:

* + יירוט- כאשר אדם לא מורשה יכול לקבל גישה לנכס
  + הפרעה- הריסת נכס
  + שינוי- מישהו נכנס לנכס ומשנה שם נתונים
  + זיוף- כאשר מישהו מתחזה, מזייף נתונים בפנים

**התקפה**- הכנסת קוד זדוני

שתי סוגי התקפות:

**התקפה פסיבית (attack passive) -** האזנות/סריקות התקשורת\* התוקף משתמש במידע, אך לא משפיע על משאבי המערכת  
- ניתוח תעבורת הרשת analysis traffic (בוב שולח לאליס הודעה, דארת' מתבונן בדפוס ההודעה)  
- פרסום מידע שעבר ברשת Release Message Content (בוב שולח לאליס הודעה, דארת' קורא את תוכן ההודעה)  
\* קשה לזהות, קל למנוע

למשל - הודעה נשלחה מצד א' לצד ב', צד ג' צפה בהודעה אך לא שידר אותה.

**התקפה אקטיבית (attack active)** - התחזות, תפיסה ושידור, זיוף נתונים  
\* התוקף משנה את משאבי המערכת ו/או את פעולתה

-התקפת מסכות Masquerade Attack (אליס מקבלת הודעה מבוב, אשר בפועל ההודעה יוצאת מדארת' וזה רק נראה כאילו זה הגיע מבוב)  
-התקפה חוזרת Replay Attack (נניח שבוב רוצה להוכיח זהותו לאליס אז הוא שולח לה את הסיסמה שלו ע"מ להזדהות. בינתיים, דארת' צותת לשיחה ושמר את הסיסמה. לאחר חילופי הדברים, דארת' מתחזה לאליס.כאשר מתבקשת הוכחת זהות, דארת' שולח את הסיסמה ששמר מהשיחה האחרונה של בוב ואליס ובכך מקבל גישה)  
-שינוי התקפה Modification Attack (בוב שולח לאליס הודעה. דארת' לוכד את ההודעה שיצאה מבוב לפני שהגיעה לאליס, ועונה במקום בוב. ז"א בוב שולח הודעה אך התשובה שאליס מקבלת כביכול מבוב היא בעצם לאחר שינוי של דארת')  
- מניעת שירותים Dos- Denial Of Services (דארת' מפריע לשירות המסופק ע"י השרת)  
התקפה שנועדה להשבית מערכת מחשב ע"י יצירת עומס חריג על משאביה. מתקפה זו תמנע גישה מקבוצת משתמש ממחשב כלשהו (שרת, אתרי בנקים, ממשלתיים וכו)   
\* קשה למנוע, קל לגלות

**בקרה**- להוציא או להקטין חולשה  
איך אפשר להגן על שרת שמחזיק קבצים שיש בהם חולשה? הזדהות כפולה(אימות דו שלבי), גישה לפי הרשאות.

איך להתגונן מהתקפות ואיומים:

* + מניעה-לחסום את ההתקפה.
  + להקשות- לגרום להתקפה להיות יותר יקרה או יותר קשה
  + הסטה- להיות פחות אטרקטיבי לתוקף
  + זיהוי- לזהות שההתקפה קורית או קרתה
  + התאוששות- להקל השפעות ההתקפה
  + דוגמא להגנה: למשל נגנבה המכונית, איך נתגונן?
  + מניעה- לא בטוח שאפשר להמנע מיזה.
  + להקשות- לשים את המכונית בחניון מוגן.
  + זיהוי- אזעקות
  + התאוששות- ביטוח

**בקרת גישה**

~קבוצות ומשתמשים  
~ אימות  
~ סיסמא: רצף קצר של תווים המשמש כאמצעי כדי לאמת מישהו.  
איך יוצרים סיסמה חזקה?

-שילוב של אותיות גדולות/קטנות, תווים מיוחדים, מספרים  
-מורכבות  
-אורך

~ הגנת קובץ  
~ רשימות שליטה –מי יכול להגשת לאיזה קובץ

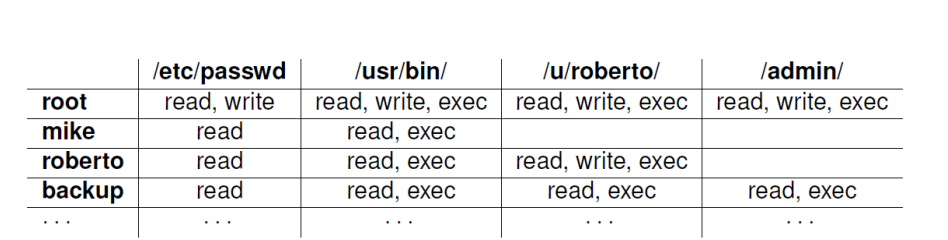
בקרת גישה בטבלה (מטריצה)

- כל שורה של טבלה זו קשורה לנושא, אשר משתמש, קבוצה או מערכת יכולים לבצע פעולות.

- כל עמודה של הטבלה משויכת לאובייקט, שהוא קובץ, ספריה, מסמך, התקן, משאב או כל ישות אחרת שעבורה אנו רוצים להגדיר גישה.

- כל תא של הטבלה מכיל זכויות גישה עבור השילוב המשויך של הנושא והאובייקט (זכויות גישה יכולות לכלול פעולות כגון קריאה, כתיבה, העתקה, ביצוע, מחיקה, והערות).

- תא ריק אומר שאין זכויות גישה מוענקות.



**קריפטוגרפיה**  
כתיבת מסרים (מוצפנים) סודיים

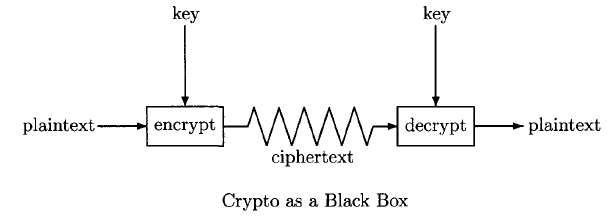
-המונחים הבסיסיים:

* קריפטולוגיה- האמנות והמדע של ביצוע ושבירת "קודים סודיים".
* קריפטוגרפיה - יצירת "קודים סודיים".
* Cryptanalysis- שבירת "קודים סודיים".
* Crypto- מילה נרדפת עבור כל הנ"ל (ועוד), כאשר המשמעות המדויקת צריכה להיות ברורה מן ההקשר.

-עוד טרמינולוגיה(מונחים):

* **צופן** או **מערכת הצפנה** משמשים ל**הצפנת** נתונים.
* הנתונים הלא מוצפנים המקוריים ידועים כ**טקסט**, והתוצאה של הצפנה היא **טקסט מוצפן**.
* אנו **מפענחים** את הטקסט המוצפן כדי לשחזר את הטקסט המקורי.
* **מפתח** משמש להגדרת הצפנה עבור הצפנה ופענוח.

מפתחות:

* **מפתח סימטרי-** אותו מפתח משמש להצפנה ולפענוח (מכאן גם הצופן נקרא צופן סימטרי), כפי שמוצג באיור הבא:
* **מפתח ציבורי\מפתח פרטי-** ההצפנה והפענוח נעשים באמצעות מפתחות שונים. מכיוון שמשתמשים במפתחות שונים, ניתן להפוך את מפתח ההצפנה לציבורי. מפתח ההצפנה ידוע **כמפתח הציבורי,** ואילו מפתח הפענוח, אשר חייב להישאר בסוד הוא **המפתח הפרטי.**

שתי סוגי הצפנות- סימטרית וא-סימטרית

**+** הצפנה סימטרית- משתמשים באותו מפתח בשביל הצפנה ופיענוח= כדי להצפין מסר X לוקחים מפתח מסויים, מצפינים את המסר, שולחים וכדי לפענח משתמשים באותו מפתח לאחור, לשחזר.

מספר אלגוריתמים בשיטה זו-

DES (data encryption standard)- פותח ב1976 ונשבר ב1991.

3DES – לא נשבר עד היום, משתמשים בבנקים, מהרגע שפותחים חשבון בנק הכל מוצפן בשיטה זו.

(advanced encryption standard) AES – נפתח ב1977 ולא נשבר עד היום. VISA

בשיטה א-סימטרית –

RES- Rivest Shamir Adelman לא נשבר עד היום

**+** הצפנה א-סימטרית- בשביל להצפין קיים מפתח ציבורי, ידוע לכולם. בשביל לפענח קיים מפתח פרטי, ידוע רק למפענח= כדי לשלוח מסר לוקחים מפתח ציבורי, מצפינים עם אלגוריתמים-יוצא איזשהו ג'יבריש. כשזה מגיע למפענח, הוא מפענח עם המפתח שרק הוא יודע.  
יתרונות בשיטה זו- מפתח לפענוח נמצא רק אצל אדם אחד ולכן קל יותר לשמור עליו ויהיה קשה מאוד לאנשים "לנחש" מהי ההצפנה.

אלגוריתם בשיטה זו-

RSA – בתהליך זה משתמשים במפתחות שונים להצפנה ולפיענוח.

בקריפטוגרפיה מה שאנחנו מחפשים לשבור זה המפתח עצמו לא הצופן. ברגע שיודעים את המפתח יודעים לפענח כל קוד באותה שיטה.

אלגוריתם הצפנה SHA

אלגוריתם ליצירת String של מספרים ואותיות על ידי הכנסה של “מידע” והמרה שלו לאותו ה String

והשימוש הכי נפוץ שלו זה לוודא שהודעה שנשלחה לא שונתה, לוודא תעודת אבטחה כך שלא שונתה(הדוגמא הקלאסית-שמירת סיסמאות באופן בטוח)

יתרון- לא ניתן לפענוח. כאשר רוצים לוודא שסיסמה אכן אמיתית משתמשים באלגוריתם SHA להצפין ובודקים אם הצופן השמור בבסיס נתונים זהה לזה שהתקבל.  
חיסרון- מכיוון שלא ניתן לפענוח קשה מאוד לדעת אם ההצפנה אכן עובדת כפי שרצו

חתימה דיגיטלית

• הצפנה של מפתח ציבורי מספקת שיטה עבור חתימות דיגיטליות

• כדי לחתום על הודעהM, , אליס פשוט מצפינה אותה עם המפתח הפרטי שלה.

• כל אחד יכול לפענח את ההודעה באמצעות המפתח הציבורי של אליס ולהשוות את התוצאה למסר M

**הצפנות קלאסיות:**

* Simple Substitution Cipher
* Double Transposition Cipher
* One-Time Pad
* ADFGVX Cipher
* The Vigenère cipher
* Playfair cipher

Simple Substitution Cipher:

במקרה זה, ההודעה תוצפן ע"י החלפת האות בn מקומות קדימה.

למשל אם n=3, ההחלפה, המשמשת כמפתח היא:



כאשר (בהסכמה) הטקסט המקורי באותיות בקטנות, והטקסט המוצפן באותיות גדולות.  
בדוגמה זו, המפתח יכול להיות נתון כ "3" שכן כמות ההזזות היא, למעשה, המפתח.  
ע"מ לפענח הצפנה מסוג זה, נחליף כל אות בטקסט המוצפן בn אותיות לאחור.

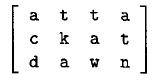
עבור n=3:



ניתן להעזר בחשיבה על אותיות שמופיעות הרבה במילים(s,e,a,i), על צמדי אותיות (ss,ee,dd.....), מילים קצרות שחוזרות הרבה (in, is, on, the...).

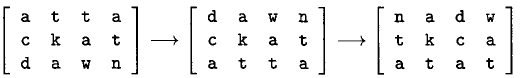
Double Transposition Cipher

במקרה זה, ע"מ להתחיל, עלינו לסדר את הטקסט שנרצה להצפין במטריצה בגודל ידוע.

למשל, הטקסט **attackatdawn:**

(מטריצה 4X3)

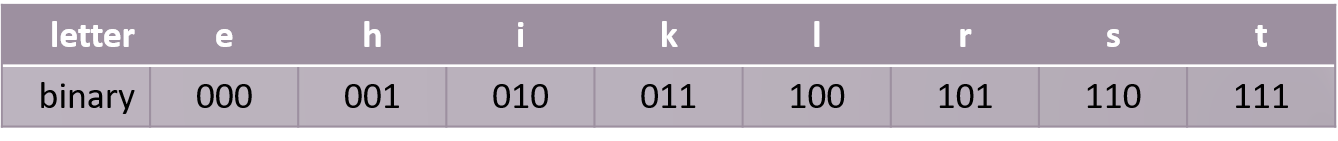
אם אנו משנים את השורות לפי (1,2,3) → (3,2,1) ולאחר מכן משנים את העמודות לפי (1,2,3,4) → (4,2,1, 3), אנחנו מקבלים



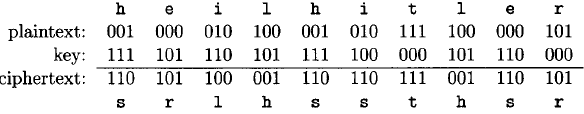
לאחר מכן, קריאת הטקסט המוצפן נקראת מהמערך הסופי: **NADWTKCAATAT**

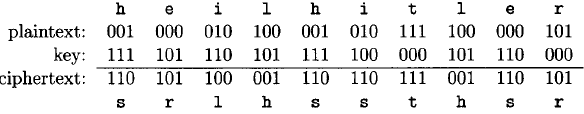
One-Time Pad:

שיטה מאובטחת ביותר.  
לשם הפשטות, הבה נבחן את האלפבית עם שמונה אותיות בלבד וייצוג בינארי שלהן.



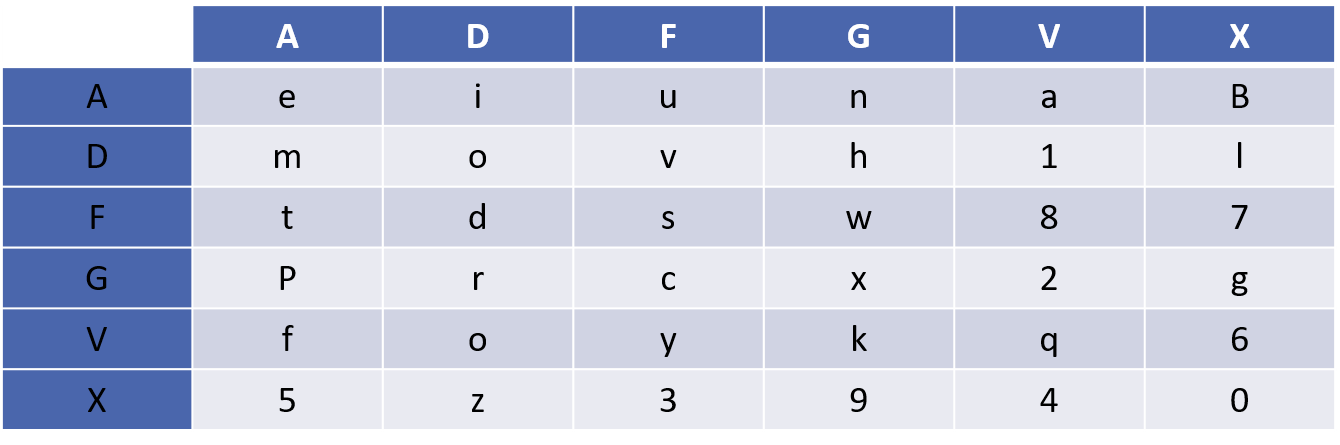
נניח רוצים להצפין את heilhilter. תחילה נמיר את אותיות התווים למחרוזת הסיביות  
**001 000 010 100 001 010 111 100 000 101**  
One-time pad מורכבת ממחרוזת סיביות שנבחרה באקראי, שאורכה זהה לאותה הודעה. המפתח הוא XORed.  
עכשיו, נניח שיש את המפתח  
110 101 110 101 111 100 101 101 110  
המהווה את האורך הנכון כדי להצפין את המסר הנ"ל, ואז כדי להצפין, נחשב כך-



נמיר חזרה את הסיביות לאותיות ונקבל צופן- srlhssthsr.  
ע"מ לשחזר את הטקסט ולפענח את הצופן נשתמש באותו מפתח   


The ADFGVX cipher:

צופן ADFGVX היה צופן שדה ששימש את הצבא הגרמני במהלך מלחמת העולם הראשונה. ADFGVX היה למעשה הרחבה של קוד מוקדם יותר בשם AGFDX.  
הצופן נקרא על שמן של שש האותיות האפשריות המשמשות בטקסט ההצפנה: A, D, F, G, V ו- X. אותיות אלה נבחרו בכוונה, משום שהן נשמעות שונות זו מזו כאשר הן מועברות דרך קוד מורס. הכוונה הייתה לצמצם את האפשרות לשגיאות.  
כללי ההצפנה:  
- הסרת רווחים וסימני פיסוק מההודעה  
- החלפת כל אות או מספר עם זוג אותיות מהכותרות  
- לבחור מילת מפתח שהמקבל יודע, לסדר אותה בשורה ובכל עמודה לשים אות מכל זוג.  
- להפוך את העמודות לפי הא,-ב של מילת המפתח  
- כל עמודה היא מילה בצופן.  
  
  
  
  
הטקסט להצפנה הוא: Attack NOW1  
הצופן: AV FA FA AV GF XG AG DD FG DV



מילת מפתח "start"

**S T A R T**

A V F A F

A A V G F

X G A G D

D F G D V

סידור לפי סדר האותיות

**A R S T**

F A A F

V G A F

A G X D

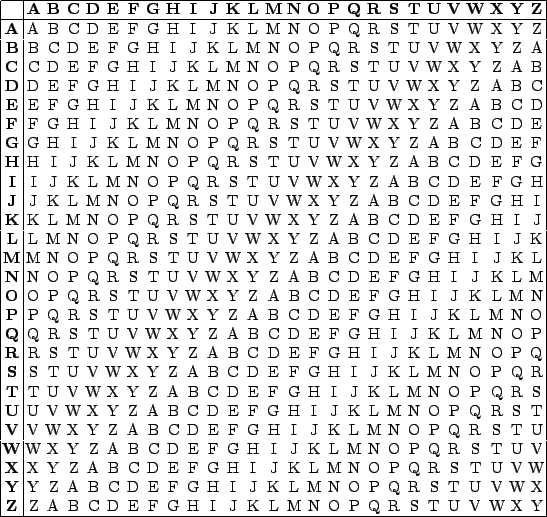
G D D V

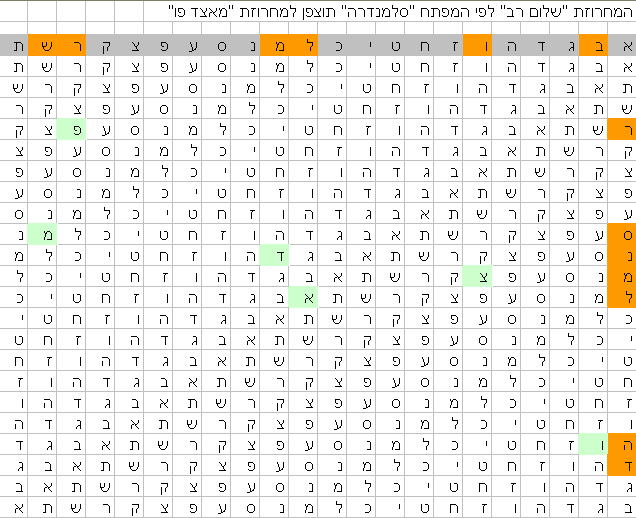
הצופן:

FVAG AGGD AAXD FFDV

The Vigenère cipher:

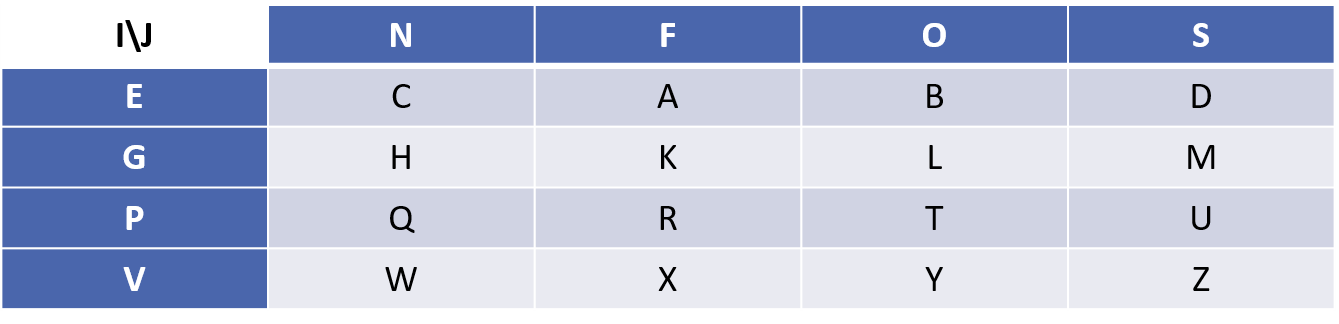
צופן Vigenère מתחיל עם מטריצה 26X26 של א'-ת'. השורה הראשונה מתחילה ב-A, שורה השנייה מתחילה ב-B וכו.



צופן זה גם דורש מילת מפתח שהשולח והמקבל ידעו.  
כל תו של ההודעה משולב עם התווים של מילת המפתח כדי למצוא את אופי הטקסט צופן

Playfair cipher:

המשתמש בוחר מילת מפתח ומכניס אותה לתאים של מטריצה 5X5.  
i, j נשארים בתא אחד. אותיות כפולות מופיעות רק פעם אחת.  
אלפבית שאינם נמצאים במילת המפתח מסודרים בתאים הנותרים משמאל לימין בשורות עוקבות בסדר עולה  
מילת המפתח INFOSEC



כללים:

* קבץ צמדים של אותיות בכל פעם
* אותיות חוזרות הפרד עם X
* לקחת זוג אותיות
* אותיות בשורות זהות מוחלפות באותיות שמימין (במחזוריות= הכוונה אם זו האות בעמודה האחרונה היא מוחלת באות בעמודה הראשונה **באותה שורה** ולא שורה למטה)
* אותיות בעמודות זהות מוחלפות באותיות שמתחת (במחזוריות)
* אותיות בעמודות ובשורות שונות מוחלפות באות שבשורה המתאימה לעמודה של האות השנייה ולהפך

לדוגמה, הטקסט המקורי: CRYPTO IS TOOY EASY  
מילת המפתח היא INFOSEC

* CR YP TO IS TO XO EA SY (טקסט מקובץ-להפריד כל זוג +אותיות חוזרות להפריד עם X)
* AQ VT YB NI YB YF CB OZ (טקסט מוצפן)

כדי לפענח, המקבל משחזר את המטריצה 5X5 באמצעות מילת המפתח ולאחר מכן משתמש באותם כללים כמו בהצפנה