Kerberos :

אימות ברשתות לא אמינות.

Digital signature:

אימות ואמינות.

SSL:

סודיות המידע – אימותים בצד שרת\לקוח.

Hashing:

יושרה ואמינות.

Cryptography:

שימוש ותירגול בטכניקות קריפטוגרפיות.

Cryptology:

לימודים משולבים של קריפטוגרפיה וקריפוטו-אנליזה.

Crypto Analysis:

ניותח שיטות קריפטוגרפיות למציאת חולשות.

Encryption:

הצפנה - התהליך להפיכת מידע לבלתי קריא ע"י שימוש בכלים ייעודיים.

Decryption –

קידוד – ההליך של הפיכת המידע מלא קריא לקריא בחזרה, ע"י שימוש בכלים ייעודיים.

Algorithm:

סט של חוקים שקובע איך יתבצעו ההצפנה והקידוד.

Key:

מפתח - פרמטר שמגדיר איך יעבוד האלגוריתם.

Key Space:

סט של כל המפתחות האפשריים .

Non – Repudiation :

וידוי הגעת המידע ליעד ווידוי שהמידע לא הוחלף או שונה בדרך.

**סוגים של הצפנות:**

1)Transposition –

האותיות בטקס (מידע) ששלחנו פשוט מחליפות מיקום לפי מפתח מסויים.

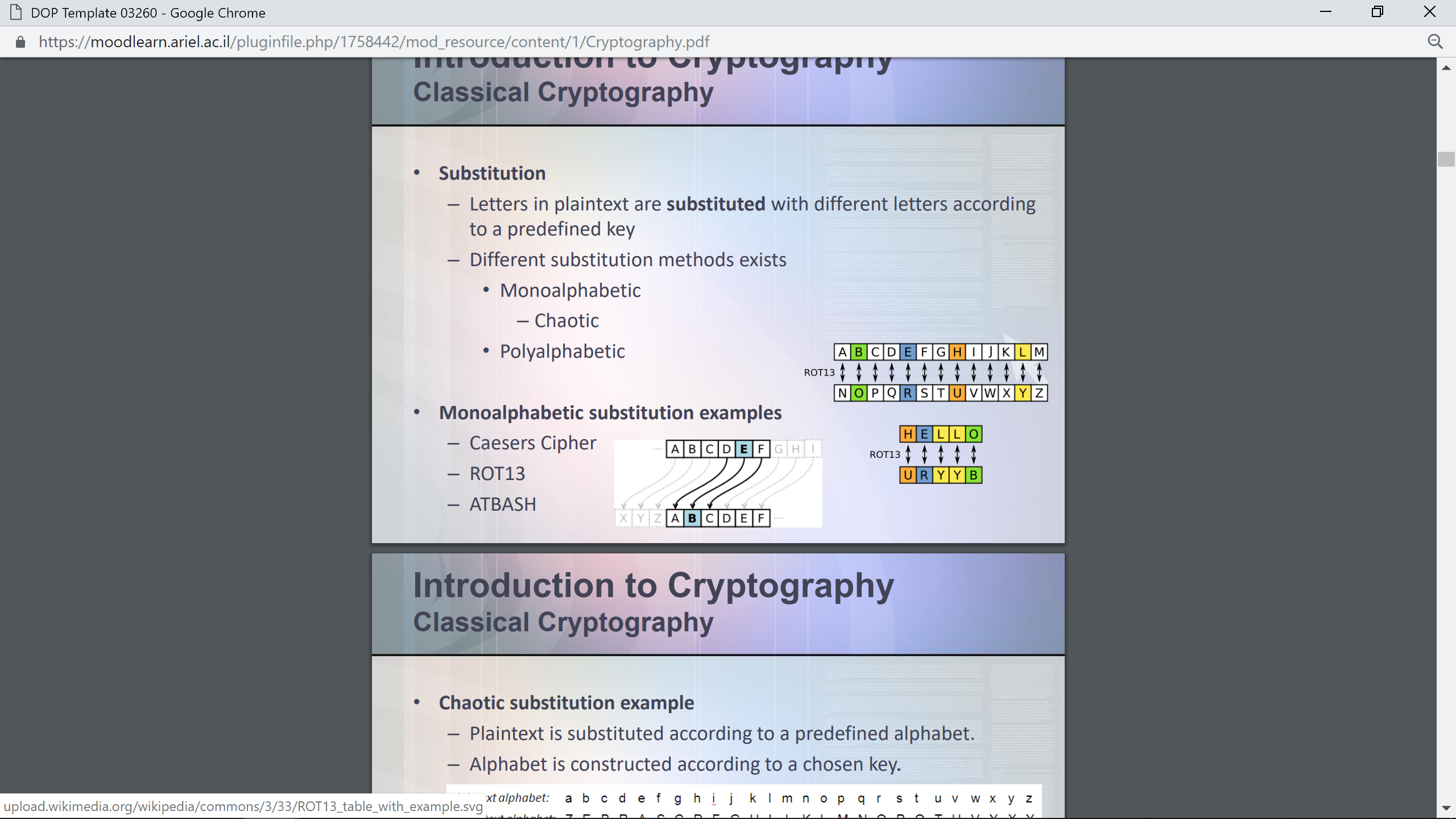
הטקסט המוצפן (CypherText) הוא בסך הכל ערבוב של הPlainText.

2)Substitution-

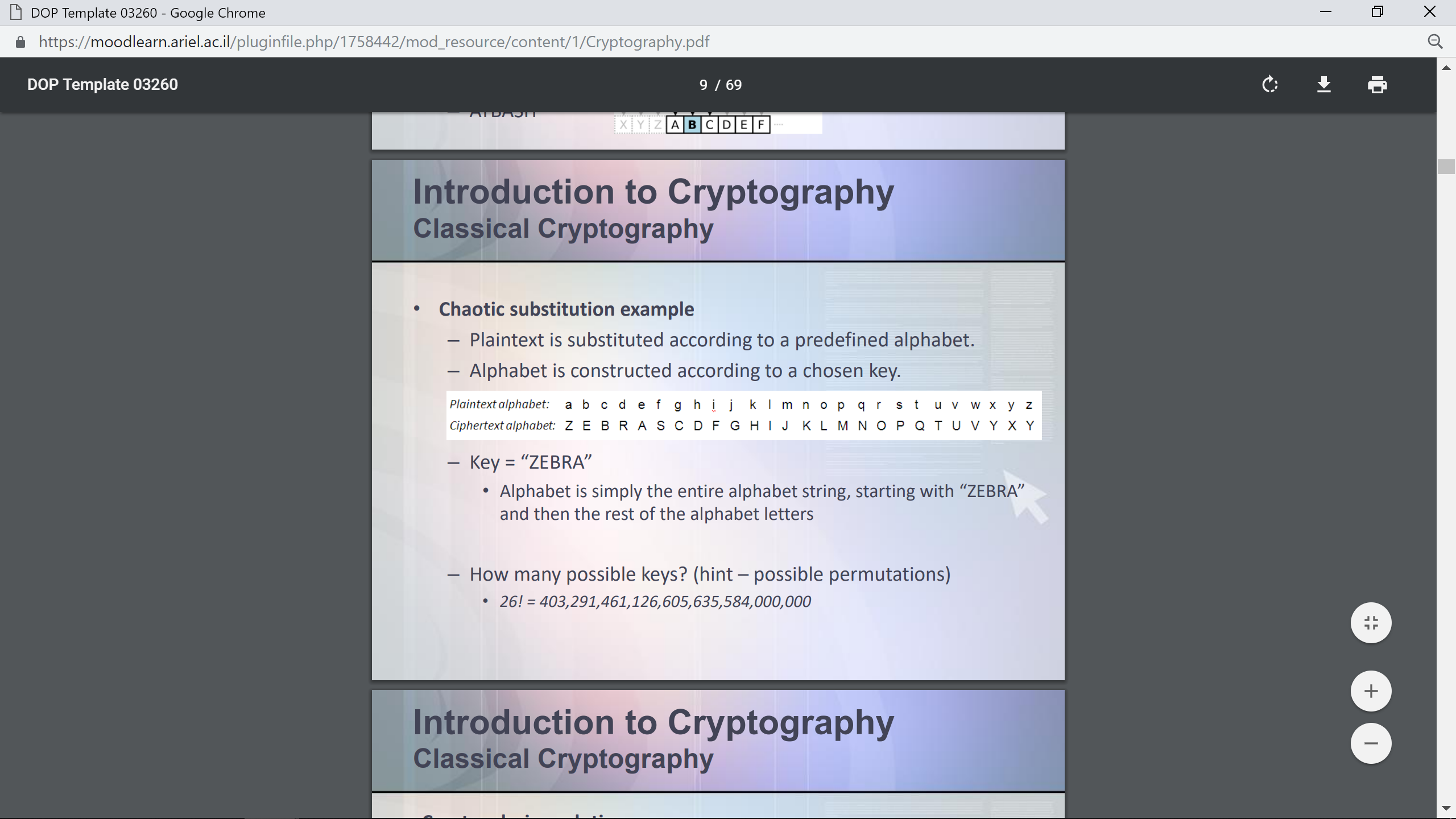
האותיות בPlainText מוחלפות באותיות \ תווים שונים המוגדרים מראש.

ישנן שיטות החלפה שונות –

1. MonoAlphabetic - - כמו צופן קיסר , אתב"ש וROT 13.

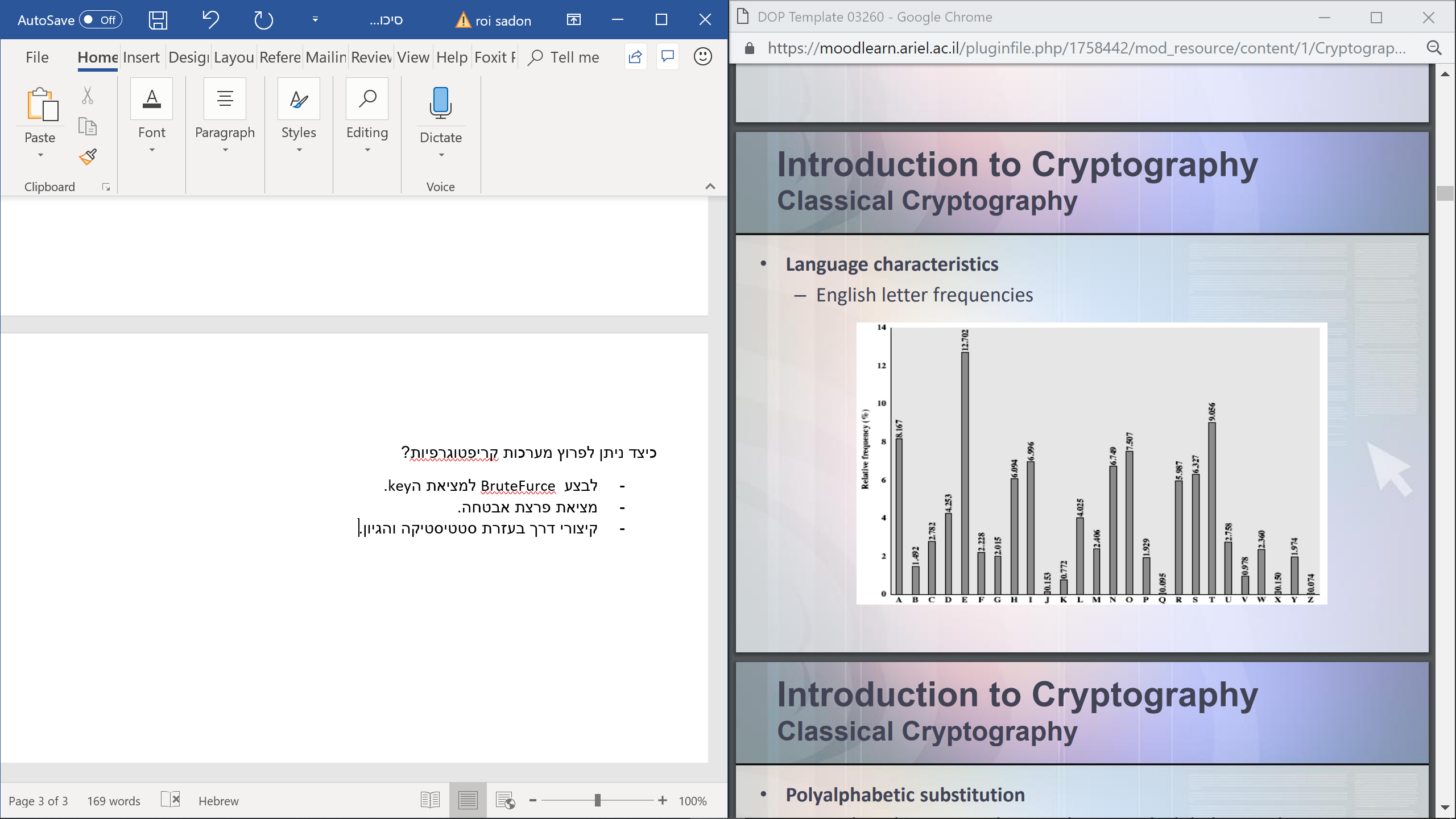


1. Chaotic – החלפת הטקסט במידע עם אותיות אחרות מגודרות מראש, ע"פ מפתח מסויים.

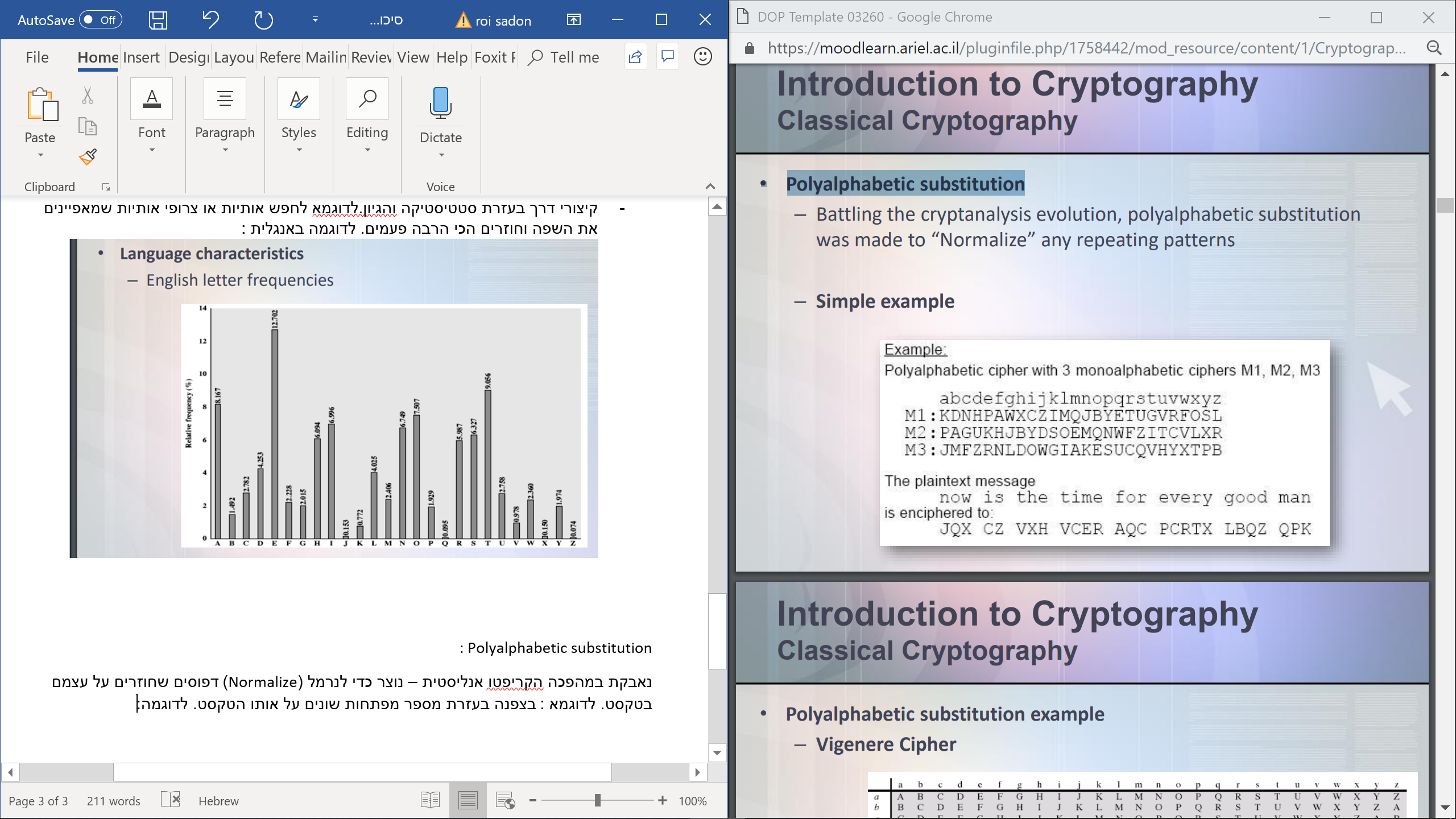


**כיצד ניתן לפרוץ מערכות קריפטוגרפיות?**

* לבצע BruteFurce למציאת הkey.
* מציאת פרצת אבטחה.

קיצורי דרך בעזרת סטטיסטיקה והגיון. לדוגמה לחפש אותיות או צרופי אותיות שמאפיינים את השפה וחוזרים הכי הרבה פעמים. בשפה האנגלית : 

: Polyalphabetic substitution

נאבקת במהפכה הקריפטו אנליסטית – נוצר כדי לנרמל (Normalize) דפוסים שחוזרים על עצמם בטקסט. לדוגמה : הצפנה בעזרת מספר מפתחות שונים על אותו הטקסט. לדוגמה: 

**:Advanced substitution examples**

צופן VERNAM: ONE TIME PAD

* בתאוריה זהו צופן בלתי פריץ.
* ללא שום קשר סטטיסטי בין אותיות.
* המפתח רנדומאלי ולעולם לא חוזר על עצמו.
* המפתח באורך הPLAIN TEXT.

חוקים בסיסים של הקריפטוגרפיה המודרנית –

* אין יותר אותיות , מספרים או סימנים אחרים.
* משתמשת עם יחידות בינאריות של 0 ו 1.
* רוב האלגוריתמים מבוססי XOR.
* מבוסס על צירופים מסובכים של החלפת אותיות ושינוי מפתחות.

**ישנן 2 סוגי הצפנות:**

1. הצפנת בלוק.

- "שובר" את הPLAIN TEXT לחתיכות (BLOCKS) בגודל ידוע.

- כל בלוק מקבל מספר ידוע מראש של סיבובים.

- מכל סיבוב מורכב מהחלפת אותיות ושינויי מפתחות.

1. הצפנה שוטפת של המידע השלם (STREAM CIPHER):

* XOR בין ביטים של מידע – וזרם אקראי של ביטים שנוצר בעזרת מפתח שהוגדר מראש.
* מעבד ביט אחד בכל פעם.
* בד"כ מהיר יותר מBLOCK CYPHER , פחות השהיות ותיקיעות.
* אם לא הושם באופן נכון עלול לגרום לפרצות אבטחה רבות.

**הצפנה סימטרית VS הצפנה לא סימטרית :**

סימטרית –

* משתמשים באותו מפתח ההצפנה גם בהצפנה וגם בקידוד של הDATA.
* אלגוריתם פחות מורכב ולכן מהיר יותר.
* משמש להצפנת דרכי תקשורת והצפנת קבצים.
* Confidentiality

**אלגוריתמים סימטרים נפוצים :**

* DES
* DES3
* AES
* RC-4
* RC-5
* Two Fish
* BlowFish
* IDEA
* CAST
* MARS
* SKIPJACK

א-סימטרית –

* משתמשים במפתח פרטי ומפתח ציבורי , כאשר הציבורי חשוף וגלוי לכולם והפרטי משמש את הבעלים של הDATA בלבד.
* האלגוריתם יותר מסובך ופועל לאט יותר.
* חלוקת מפתחות ציבוריים וחתימה דיגיטלית.
* Authentication and non repudiation (אימות וודיוי הגעת המידע ליעד) כדי למנוע הכחשה של קבלת המידע .
* כל סט של מפתחות פרטי וציבורי הוא ייחודי.

**אלגוריתמים א-סימטרים נפוצים :**

* DSA
* RSA
* ECC – יעיל מאוד אך נועד לעבוד רק בסביבות מסויימות.
* EL GAMAL
* DIFFIE HELMAN - האלגוריתם הא-סימטרי הראשון. הסכמה על מפתח הצפנה בלי שיתוף מידע.
* KNAPSACK

Initialization Vector (IV)

* ערכים רנדומאליים נכנסים לתוך הטקסט המוצפן כדי לוודא שאין דפוסים שחוזרים על עצמם בהצפנה.

Hybrid Cryptography In SSL and TLS:

* הלקוח מבצע חיבור מאובטח.
* צד השרת מגיב ושולח את המפתח הציבורי שלו ללקוח.
* הלקוח יוצר מפתח הפעלה סימטרי.
* ההצפנה של הלקוח משתמש במפתח הציבורי של השרת כדי להצפין את מפתח ההפעלה.
* הלקוח שולח את מפתח ההפעלה שמוצפן בעזרת המפתח הציבורי של הסרבר .
* הסרבר משתמש במפתח הפרטי שלו כדי לקודד את הפרטים.
* כעת כאשר מפתח ההפעלה הסימטרי הופץ, לשני הצדדים יש דרך תקשורת מאובטחת .

INTEGRITY :

* מידע נערך בטעות או בדרך של שחיתות.
* MAC - מספק וידוי אימות ויושרה במידה מסוימת אך לא חזקה מספיק כדי להיות NON REPUDTATION, מכוון שהוא משתמש במפתח סימטרי.
* DIGITAL SIGNATURE - יכול לאתר גם מתקפות וגם שינוים שקרו בטעות , מספקת NON REPUDATION.

HASHING:

* הצגה דיגיטלית של תוכן הקובץ.
* אם הקובץ השתנה , גם ההאש ישתנה.
* מתמטיקה חד כיוונית.
* כאשר שתי מסמכים שונים מייצרים את אותו ההאש , זה נקרא collision(התנגשות).
* מתקפות יומולדת הם נסיונות לגרום להתנגשויות שכאלו, זה מתבסס על הרעיון שזה קל ומהיר יותר למצוא שני האשים שבמקרה תואמים , מאשר לנסות ולהפיק את ההאש הספציפי.

HASHING ALGORITHM:

* הודעה באורך משתנה.
* 5-MD היה הסטנדרט עם 128 ביט האש.
* SHA - 1 - 160 ביט, החליף את MD5 ברוב החלקים.
* SHA 256 - הפך לאחרונה לנפוץ במיוחד.
* RiperMD, Tiger,, Whirlpool ו -HAVAL הם אלגוריתמי האש פחות מוכרים.

WEP SECURITY FEATURES:

* המידע שמגיע אמין ובטוח.
* כל PACKET מוצפנת באמצעות - RC4מפתח של 64 או 128 ביטים.
* לכל PACKET מצורף INITIALIZATION VECTOR בגודל של 24 ביט.

BREAKING WEP : חדירה לWEP:

* הזרמת תעבורה ברשת(הזרקות שווא).
* הקלטת תעבורת הרשת.
* שימוש במתקפות סטטיסטיות על המידע שהזרמנו ברשת , אחרי 40 אלף PACKETS שהזרקנו יש בערך 50% הצלחה בפריצה , ואחרי 85 אלף 95% הצלחה!

אלגוריתם RSA :

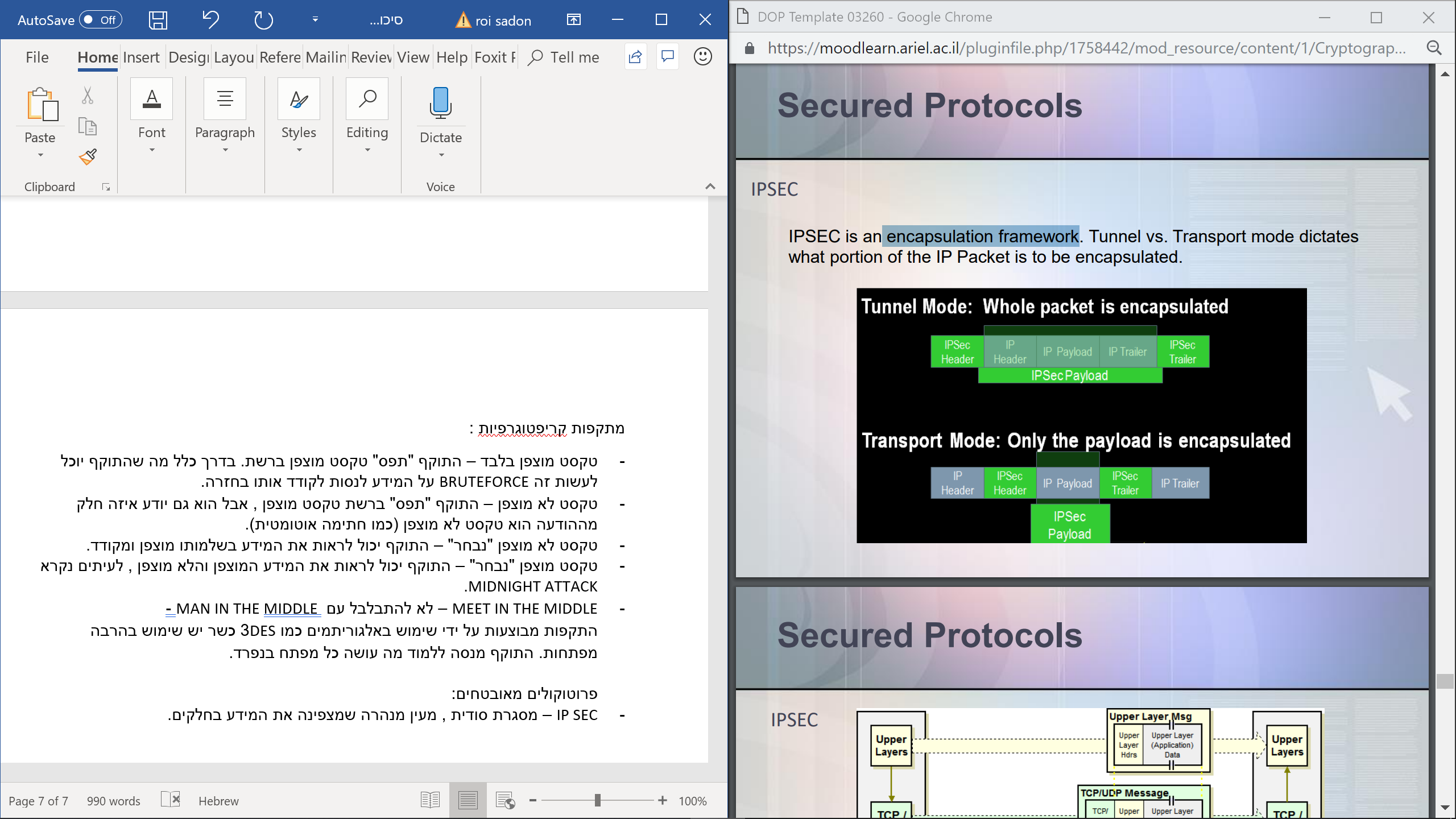
* מתבסס על ייצור של 2 מספרים ראשוניים.
* קל לחישוב .
* קשה מאוד לפירוק חזרה לגורמים.

**מתקפות קריפטוגרפיות :**

* טקסט מוצפן בלבד – התוקף "תפס" טקסט מוצפן ברשת. בדרך כלל מה שהתוקף יוכל לעשות זה BRUTEFORCE על המידע לנסות לקודד אותו בחזרה.
* טקסט לא מוצפן – התוקף "תפס" ברשת טקסט מוצפן , אבל הוא גם יודע איזה חלק מההודעה הוא טקסט לא מוצפן (כמו חתימה אוטומטית).
* טקסט לא מוצפן "נבחר" – התוקף יכול לראות את המידע בשלמותו מוצפן ומקודד.
* טקסט מוצפן "נבחר" – התוקף יכול לראות את גם המידע המוצפן וגם מפוענח , לעיתים נקרא MIDNIGHT ATTACK.
* MEET IN THE MIDDLE – לא להתבלבל עם MAN IN THE MIDDLE -

התקפות מבוצעות על ידי שימוש באלגוריתמים כמו DES3 כאשר יש שימוש בהרבה מפתחות. התוקף מנסה ללמוד מה עושה כל מפתח בנפרד.

**פרוטוקולים מאובטחים:**

* IP SEC – מסגרת סודית , מעין מנהרה שמצפינה את המידע בחלקים.
* 

**פרוטוקולי משנה של IPSEC –**

* AH (AUTHENTICATION HEADER) – מספק יושרה , אמינות , ווידוי הגעת המידע ליעד באמצעות שימוש בICV (INTEGRITY CHECK VALUE). הICV רץ על הפאקטה כולה חוץ מחלקים דינאמים בHEADER. אין סודיות !!!
* ESP - (Encapsulating Security Payload) = הצפנת מטען מאובטח – מספקת אמינות ויושרה דרך MAC.
* IKE – INTERNET KEY EXHANGE = החלפת מפתחות אינטרנטיים – אין שירותי ביטחון, רק ניהול של חיבור מאובטח.
* ISAKMP - (Internet Security Association and Key Management Protocol).
* SSH – (SECURE SHELL) – חלופה מאובטחת לפרוטוקולים מנהליים.
* PGP – PREETY GOOD PRIVACY
* S\MIME