עבודת גמר קריפטוגרפיה

דור לבקוביץ – 203565015

.1

א)

CAESAR – Sync

VIGENERE – Sync

ATBASH – Sync

DES – Sync

AES – Sync

מערכת סימטרית משתמשת במפתח פרטי ואילו מערכת אסימטרית משתמשת גם בציבורי וגם בפרטי.

ב) המפתח הקצר ביותר מבין הצפנים המוזכרים מעלה הוא צופן CAESAR משום שאורכו של המפתח קצר יותר מהמסר שלו.

ג) צפני החלפה עובדות באלגוריתם שמה שהן עושות בעצם זה שהן משנות סדר אותיות (לדוגמה צופן קיסר ייקח את האות B ויחליף אותה עם האות E). צפני התמרה לעומת זאת עובדות בצורה שונה למשל האות שמופיע הכי הרבה פעמים ולהשוות למילים נפוצות וכו'.

2. אי אפשר לדחוס נתונים שהוצפנו ולכן יש קודם לדחוס את החומר ורק לאחר מכן להצפין מה שיוצר הצפנה טובה ויעילה יותר.

4. התשובה היא כל אותיות הא-ב בעצרת. (22 עצרת = 1,124,000,727,777,607,680,000)

10. PRG לא יכול לחזור על עצמו כי אם הוא יחזור על עצמו הוא לא יהיה בטוח כבר.

11. כאשר האפסילון קטן מ- $1/2^{80}$ ה- PRG בטוח יותר.

12. אלגוריתמים של כל PRP צריך להיות שונה מהשני כדי להיות בטוח אחרת נחשב כלא בטוח לשימוש.

.13

א) האפסילון נחשב בטוח כך אבל עדיף שיהיה קטן ככל שאפשר על מנת לחזק את הבטיחות שלו.

ב) PRG בלתי צפוי נחשב כבטוח יותר.

ג) PRF יוצר מספרים רנדומלים ו- PRP משנה את סדר המספרים.

ד) PRP אינו יכול להיות PRF משום שהם לא עובדים בצורה דומה.

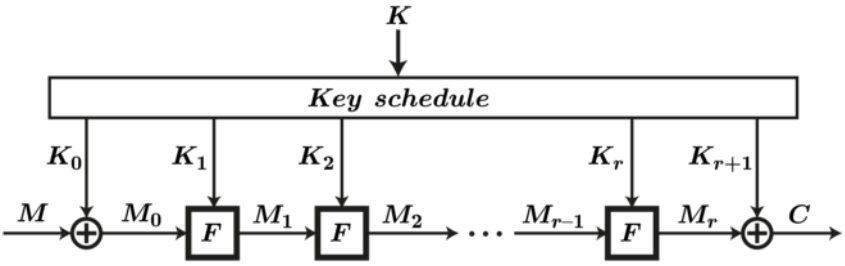
ה) 3DES עושה שימוש ב- PRG.

14. OTP חייב להיות באורך המילה בנוסף לפי האלגוריתם שלו אסור שיחזור על עצמו כי יחשב כלא בטוח.

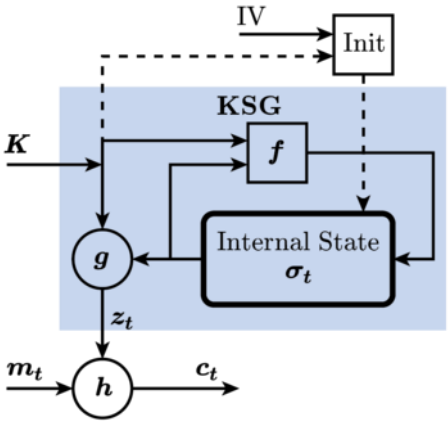
15. DES 3 בטור לא מקיימים את התנאי בשאלה

16. צופן DES ב56 סיביות(2^{56*8}) וזה מספר המפתחות האקראיים להבדיל מ- AES שמשתמש ב- 192 סיביות(2^{192*8}) מפתחות אקראיים.

17. Block Ciphers - **צופן בלוקים הוא פרימיטיב קריפטוגרפי סימטרי** הפועל על מחרוזת סיביות באורך קבוע הנקראת **בלוק** באמצעות טרנספורמציה קבועה.



Stream Cipher - צופן זרם הוא סוג של צופן סימטרי שמצפין זרם באורך משתנה של יחידות מידע תוך שימוש בטרנספורמציה המייצרת מפתח לפי 'מצב פנימי' של הצופן.



18. MAC – MAC הוא שם כולל לפונקציות עם מפצח סודי המתקבל מפתח סודי ומסר באורך שרירותי ומפיקה פיסת מידע קצרה הנקראת Authenticator. הוא עובד עם שניהם אבל כיום משתמשים יותר ב- PRP כי הוא פחות פריץ.

19. ערכו צריך להיות קטן יותר $1/2^{80}$.

20. CA משתמש הן במפתחות פרטיים והן בציבוריים

.22

א) CERTIFICATE AUTHORITY

ב) יובל מעביר לאבנר את המספר 27

ג) אבנר מעביר יובל את המספר 48

ד) המספר שהתקבל מהחישוב הינו: 174 משמע שהמפתח שנוצר זוגי

.23

א) M=9

ב)

.a

Z – 2035650159

N – a2e33d344f

.b

Z - 1111001010101011000111001101111

N - 1000000011001100000011010001110100

Res – 1010001010011010011010001011101000100000

מה שיצא לי בסעיף א' הוא 9 שאותה הוספתי לסוף התעודת זהות שלי, לקחתי את N שלי ועשיתי XOR(כל שתי אותיות שונות נותנות 1 אחרת יינתן 0) לשניהם בבינארית .