8 בספטמבר 2021

אבטחת מידע 10313

פתרון תרגיל 3

מרצה: ד"ר עמית קליינמן

בודק: ערד פלד

1. שורשים פרימיטיביים

Exponents of 1 are all 1

$2^1=2$, $2^2=4$, $2^3=8$, $2^4 \equiv 5$, $2^5 \equiv 10$, $2^6 \equiv 9$, $2^7 \equiv 7$, $2^8 \equiv 3$, $2^9 \equiv 6$, $2^{10} \equiv 1 \pmod{11}$

Exponents of 2 are 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 (primitive root!)

$3^1=3$, $3^2 \equiv 9$, $3^3 \equiv 5$, $3^4 \equiv 4$, $3^5 \equiv 1 \pmod{11}$

Exponents of 3 are 3, 9, 5, 4, 1 (then repeat)

Exponents of 4 are 4, 5, 9, 3, 1 (then repeat)

Exponents of 5 are 5, 3, 4, 9, 1 (then repeat)

Exponents of 6 are 6, 3, 7, 9, 10,5, 8, 4, 2 (primitive root!)

Exponents of 7 are 7, 5, 2, 3, 10, 4, 6, 9, 8 (primitive root!)

Exponents of 8 are 8, 9, 6, 4, 10, 3, 2, 5, 7 (primitive root!)

Exponents of 9 are 9, 4, 3, 5, 1 (then repeat)

Exponents of 10 are 10, 1 (then repeat)

See: https://www.mathcelebrity.com/primitiveroot.php

2.

א. CBC = cipher block chaining, זהו אופן פעולה אשר בו שרשרת של בלוקי צופן נוצרת כך שבלוק צופן תלוי בהצפנה נאותה של הבלוק המוצפן הקודם. התלות הפנימית הזאת מבטיחה ששינוי בביט כלשהו בהודעה הגלוייה יגרום לבלוק המוצפן הסופי להשתנות בצורה שאינו נתנת לניבוי או לפעולה הפיכה ללא ידיעת המפתח בו נעשה שימוש עבור מצפין הבלוקים.

ב. שלושת מטרות האבטחה המתאימות הינן:

- **Authentication** - the act of confirming the truth of an attribute of a single piece of data (a datum) claimed true by an entity, e.g., it can be a security measure designed to establish the validity of a transmission, message, or originator. Multiple authentication factors (inherence, knowledge or ownership) are used to enhance security of a transaction. Authentication protects against impersonation.
- **Integrity** - Quality of an IS (Information System) that reflects: The logical correctness and reliability of the operating system. The logical completeness of the hardware and software implementing the protection mechanisms; and The consistency of the data structures and occurrence of the stored data.

- Integrity protects against unauthorized modification or destruction of operating system, hardware and software implementing the protection mechanisms, and the data.

- **Non-repudiation** - ensure that a party to a contract or a communication cannot deny the transaction. It protects against denying of a transaction.

ג. IV = initialization vector זהו קלט באורך קבוע לפרמיטיב קריפטוגרפי (במקרה זה פונקציית ה-XOR).

ד. CBC-MAC(M, K) = EK(EK(EK(m1 ⊕ O) ⊕ m2) ⊕ m3)

ה. בוב צריך לחזור על חישוב ה-CBC-MAC(M,K) כפי שבוצע בתת-הסעיף הקודם ולהשוות את התוצאה לחתימה שהוא קיבל מאליס. אם התוצאות שוות, ההודעה מאומתת.

.3

א. הצפנה א-סימטרית

ב. הבחירה ב RSA כיוון שהוא מספק הן אוטנטיקצייה והן שמירה על סודיות. מטרת האבטחה הנוספת היא אוטנטיקצייה.

ג. Modulus n ו- $\phi(n)$, מחושבים להלן: $n = p \cdot q = 23 \cdot 5 = 115$

$\phi(n) = (p-1) \cdot (q-1) = 22 \cdot 4 = 88$

e זר ל $\phi(n)$ – כיון ש $\gcd(19,88)=1$

ד. המפתח הציבורי = (19, 115)

ה. חישוב המפתח הפרטי:

$d \cdot 19 \equiv 1 \pmod{88}$ => $d \cdot 19 = 1 + k \cdot 88$ => $19 \cdot d + 88 \cdot K = 1$

נפתור ע"פ אלגוריתם אוקלידס המורחב:

q	r	j	k
-	88	1	0
-	19	0	1
4	12	1	-4
1	7	-1	5
1	5	2	-9
1	2	-3	14
2	1	8	-37
2	0		

$d = -37 + \Phi(n) = -37 + 88 = 51$

d = 51; k = -11

1st line is: -, a, 1, 0

2nd line is:-, b, 0, 1

3rd line and thereafter - calculated according to the 2 lines above it:

$q_i = r_{i-2} / r_{i-1}$ (the quotient)

$r_i = r_{i-2} \bmod r_{i-1} = r_{i-2} - q_i\, r_{i-1}$ (the reminder)

$j_i = j_{i-2} - q_i\, j_{i-1}$

$k_i = k_{i-2} - q_i\, k_{i-1}$

המפתח הפרטי = (51,115)

ו. כן, קיים קשר מתמטי בין e של המפתח הציבורי ו d של המפתח הפרטי, שכן הם נוצרו ביחד על מנת לאפשר פיענוח בעזרת d מסר מוצפן שהוצפן ע"י e. חלקי המפתח e, d מקיימים את המשוואה: $e \cdot d \equiv 1 \bmod \Phi(n)$

ז. באלפבית 22 אותיות $n > 22 = 22^1$ $n < 484 = 22^2$ לכן יחלק את ההודעה בת ה 2 תווים לשני בלוקים בני תו בודד.

21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

א = 0, ש = 20, ל = 11, מ = 12, ט = 8, ר = 19 ו- ה = 4

כל בלוק M יוצפן ע"פ הנוסחה: $M^{19} \bmod 115$, **$19 = (10011)_2$**

$0^7 \bmod 115 = 0$ <= מתאים למחרוזת **אא**

$20^{19} \bmod 115$

1) (bit=1): $20 \bmod 115 = 20$
2) (bit=2): $(20^2) \bmod 115 = 55$
3) (bit=3): $(55^2) \bmod 115 = 35$
4) (bit=4): $20\ (35^2) \bmod 115 = 5$
5) (bit=5): $20\ (5^2) \bmod 115 = \mathbf{40}$

$40 \div 22 = 1$ Rem 18

$\Rightarrow 40 = 1 \cdot 22^1 + 18 \cdot 22^0$

מתאים למחרוזת: קב

המסר המוצפן הינו: אאקב

ח. באלפבית 22 אותיות mod n יכול לתת תוצאות עד 114. $22^2 = 484 > 114 > 22^1 = 22$, כלומר בטקסט המוצפן הבלוקים הם בגודל 2 אותיות וכיוון שהמסר המוצפן הוא באורך 4 תוים => יהיו 2 בלוקים.

ט. הפונקצייה המתמטית שתפעיל כדי לפענח את ההודעה היא: $B^{223} \bmod 583$

4. פונקציות גיבוב:

א. משום שבמקרה שמסד הנתונים המכיל את סיסמאות המשתמשים נפרץ, הפורץ לא ישיג את ססמאות המשתמשים אלא רק את ערכי הגיבוב שלהם שאינם הפיכים.

ב. למרות שערכי גיבוב אינם הפיכים, ללא המלחה, התוקף יכול להריץ התקפת מילון, להשתמש בטבלאות חיפוש או בטבלאות קשת ו"לשבור" את ערך הגיבוב של הסיסמה.

ג. חיפוש בגוגל מראה שכפי הנראה "Security1" אינה סיסמה טובה (הינה סיסמה חלשה).