Examen - Criptografie si Securitate

Nume si prenume: Anei Alexandra-Gabriela

Grupa: 332

Subiecte netratate: 2d), 3f)

Anei Alexandra-Gabriela, grupa 332

20.05.2020

Anei Alexandra-Gabriela
Grupa 332

Examen Criptografie

1) a) Știm că cheia k trebuie să fie la fel de lungă precum mesajul. În momentul în care XOR-ăm un mesaj de lungime n cu o cheie de aceeași lungime un mesaj criptat tot cu lungimea n. Deci $|K| = |C| = |M|$.

b) $c' = m \oplus k$

știm că $k = m \Rightarrow c' = m \oplus m$

$\Rightarrow c' = 0$

Nu putem decripta. Schema OTP este perfect sigură, nu cunoaștem nimic despre cheie și nici despre mesajul dar.

2) a) $c = c_1 \| c_2 \| c_3$

$c_i = F_k((ctr+i) \oplus m_i),\ i = \overline{1,3}$ și $m = m_1 \| m_2 \| m_3$

$\Rightarrow c = F_k((ctr+1) \oplus m_1) \| F_k((ctr+2) \oplus m_2) \| F_k((ctr+3) \oplus m_2)$

b) F_k trebuie să fie inversabilă

$c_i = F_k((ctr+i) \oplus m_i)$

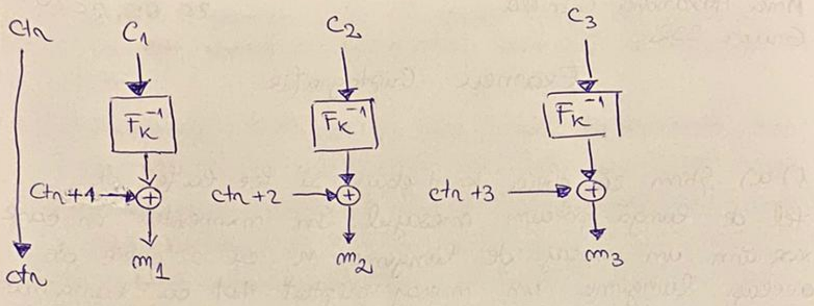
$\Rightarrow F_k^{-1}(c_i) = (ctr+i) \oplus m_i$

$(ctr+i) \oplus F_k^{-1}(c_i) = \underbrace{(ctr+i) \oplus (ctr+i)} \oplus m_i$

$\Rightarrow (ctr+i) \oplus F_k^{-1}(c_i) = 0 \oplus m_i$

$\Rightarrow m_i = F_k^{-1}(c_i) \oplus (ctr+i)$

Anei Alexandra-Gabriela, grupa 332



c) Verificăm corectitudinea sistemului cu relația

$Dec_K(Enc_K(m_i)) = m_i$

$Enc_K(m_i) = \cancel{m \oplus k}\ F_K((ctr+i) \oplus m_i)$

$Dec_K(c_i) = \cancel{c \oplus k}\ F_K^{-1}(c_i) \oplus (ctr+i)$

$\cancel{\Rightarrow Dec_K(Enc_K(m)) = Dec_K(m \oplus k) = \underbrace{(m \oplus k) \oplus k}_{0} = m \oplus 0 = m}$

~~=> Sistemul este corect~~

$Dec_K(Enc_K(m)) = Dec_K(F_K((ctr+i) \oplus m_i)) =$

$= F_K^{-1}(F_K((ctr+i) \oplus m_i)) \oplus (ctr+i) = (ctr+i) \oplus m_i \oplus (ctr+i)$

$= m_i$ => sistemul este simetric

În cazul în care paddingul nu se realizează, sistemul este corect.

În cazul în care avem lungimea mesajului clar este ~~divizibila~~ multiplu de număr de blocuri alocate și totuși facem padding, la decriptare obținem același mesaj cu padding și nu este afectată semnificația mesajului, paddingul fiind redundant.

În cazul în care facem padding pentru că avem ultimul bloc cu mai puțini biți decât restul, există șansa să fie afectată semnificația

Anei Alexandra-Gabriela, grupa 332

mesajului, pentru că cel care face decriptarea nu va ~~ști~~ cunoaște lungimea inițială a blocului respectiv.

~~2 d) Sistemul CTRmodif este unul determinist, deci nu este CPA-sigur, automat nu este nici CCA-sigur. Adversarul cere oracolului de criptare criptarea mesajului m_0. Dacă textul criptat este egal cu c, atunci $b'=0$, altfel $b'=1$. În concluzie, adversarul câștigă cu probabilitate 1~~.

e) Dacă lungimea blocului = 48, securitatea sistemului este redusă, deoarece timpul de execuție al unei încercări de decriptare este foarte scurt. Securitatea depinde mult de lungimea ~~mesajului~~ blocului, fiind mult mai simplu să decriptezi blocuri de 48 biți față de 256 biți (standardul curent).

3) a) MD5 este o funcție hash rapidă. Practic, o parolă criptată cu MD5 se poate decripta foarte ușor de un telefon mobil ($\approx$ în 30 s). În practică, se folosesc funcții hash lente pentru a stoca parole. Adăugând valori salt în criptarea cu MD5 doar îngreunăm decriptarea, nu o facem imposibilă. Să presupunem birthday attack: sunt necesare $\approx 2^{64}$ evaluări doar pentru decriptarea unei parole stocată cu MD5. Dacă valoarea salt are doar 8 biți vor fi necesare $\approx 2^8 + 2^{64}$ evaluări pentru decriptarea parolei. Dacă valoarea salt este prea mare, se va ocupa mult prea mult spațiu de stocare în baza de date, deci este o metodă nefiabilă. Așadar, adăugând o valoare salt criptării aduce un plus de siguranță, dar sistemul nu devine 100% sigur, din cauza funcției MD5, care este foarte nesigură.

3/6

Anei Alexandra-Gabriela, grupa 332

b) $G(x) = x^2 \bmod x = 0$

~~nu este satisfăcută proprietatea de expansiune~~

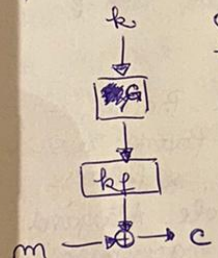
~~$\forall n, \ell(n) \geq n$ unde $|x| = n$~~

~~de exemplu, am $x = 10101010 \Rightarrow n = 8$~~

Oricare ar fi x, este generat 0, deci secvența de ieșire este mai scurtă decât cea de intrare (de exemplu $x = 10000$) $\Rightarrow$ nu este satisfăcută proprietatea de expansiune $\Rightarrow$ nu este PRG.

În plus, generând mereu 0, nu sunt generate valori aleatoare.

c) Folosindu-mă de schema unui sistem fluid



avem relația $c = kf \oplus m$

kf este generat de $G \Rightarrow$

$c = G(F(MD5(pw, salt))) \oplus m$

dar, $G(x) = 0, \forall x$

$\Rightarrow c = 0 \oplus m$

$\Rightarrow c = m$

d) $f(n) = \frac{1}{n^{65537}}$ nu este neglijabilă deoarece există $p(n) = n^{65538}$ și $\lim\limits_{n \to \infty} p(n) \cdot f(n) = \infty$

$\Rightarrow$ DLP nu e dificilă $\Rightarrow$ sistemul este nesigur

e) Protocolul rămâne vulnerabil la atacul Man-in-the-Middle. Se poate împiedica atacul cu un sistem de autentificare sau cu o signatură digitală

g) Se încalcă principiul lui Kerckhoffs: Sistemul nu trebuie să fie secret, poate să cadă ușor în mâinile adversarului, adică securitatea unui sistem trebuie să ~~cons~~ aibă la bază doar menținerea secretă a cheii. În cazul nostru, o parte din sistem este secret, adică ~~MACAuth~~ AuthMAC-ul.

h) Confidențialitatea, pentru că secretul informației nu este păstrat, conform punctului 2c), ~~deci~~ mesajul criptat = mesajul clar.

Autentificarea, pentru că doar managerii beneficiază de AuthMAC, nu toată firma.

4) a) $N = p \cdot q$, p și q prime

Cu ajutorul unui convertor online (hex to decimal), am observat că ultimele cifre ale lui N sunt 296.

$N \vdots 8 \Rightarrow p$ sau/și q nu sunt prime $\Rightarrow$ Sistemul nu este corect definit.

b) $y^2 = x^3 + 17x + 3 \pmod{29}$

$(8,10) \in$ curbei eliptice $\begin{cases} 10^2 = 8^3 + 17 \cdot 8 + 3 \pmod{29} \\ 13 = 13 \end{cases}$

$(8,11) \notin$ curbei eliptice $11^2 \bmod 29 \neq 13$
$\Rightarrow$ nu are invers

inversul lui $(8,10) = (8, -10 \bmod 29) = (8, -19)$

Anei Alexandra-Gabriela, grupa 332

c) Metoda de criptare pe baza unei curbe eliptice este foarte bună din punct de vedere al securității deoarece pentru o valoare modulo foarte mare există foarte multe puncte în plotarea curbei. Dar, curba dată este slabă din punct de vedere al securității deoarece are valoarea modulo = 29. Se recomandă o valoare modulo $>= 2^{160}$ și să fie primă.

d) $y^2 = x^3 - 3x + b \pmod{p}$

p = 115792089210356248762697446949407573530086 1434152903141955363130886709785395 1

b = 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b (hexazecimal)

Curba P-256, ~~găsită~~ recomandată de NIST.