În încercarea de a rezolva misterele universului —

① cheie criptare 80 biți

a) Câte chei posibile există: 2^{80} ($\{0,1\}$)

b) Cât timp necesită determinarea cheii dacă se pot efectua 2^{20} criptări pe secundă?

$\frac{2^{80}}{2^{20}} = 2^{80-20} = 2^{60}$ secunde

c) Este atacul fezabil?

Evident nu → durează câteva ~~ore~~ secole

② padding OAEP, $OAEP(m,r) = x_1 \| x_2$ unde:

$x_1 = m \| 0^{n/2} \oplus G(r)$

$x_2 = r \oplus H(r)$ unde

$m \in \{0,1\}^{n/2}$, r - val. aleat pe n biți. G și H - fct. hash pe n biți.

Determinați $OAEP^{-1}$ adică cunoscând $OAEP(m,r) = x_1 \| x_2$, indicați cum se calculează m.

$OAEP(m,r) = x_1 \| x_2$ ← concatenare

Observăm că numai x_1 are m (pe care trebuie să-l aflu)

$x_1 = m \| 0^{n/2} \oplus G(r)$.

Ca să îl aflu pe m xorez încă odată cu $G(r)$ și iau primii $n/2$ biți. i.e:

$X_1 = m \| 0^{n/2} \oplus G(r) \oplus G(r) \Rightarrow X_1 = m \| 0^{n/2}$

↓ cat d.

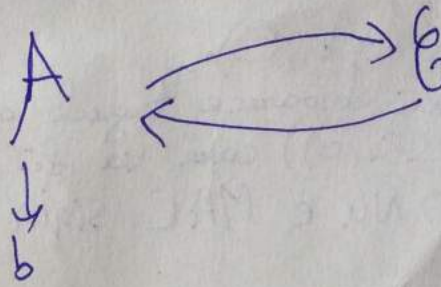
③ (Enc, Dec) - sistem criptare simetric.

Se consideră sistemul de criptare (Enc', Dec') pt. mesaje de dimensiune dublă cu funcția de criptare definită astfel:

$Enc'_k(m_1 \| m_2) = (Enc_k(m_1), Enc_k(m_2))$.

Arătați că sistemul nu este CCA sigur.

CCA → am acces la oracol de criptare și decriptare



Atenție!

Enc' → reprezintă criptarea unui mesaj cu două componente (lungime dublă)

Fie mesajul $m_i = m_0 \| m_1$

$m_j = m_2 \| m_3$.

Trimit spre criptare $m_i \to Enc'(m_0, m_1) = Enc_k(m_0), Enc_k(m_1)$

$m_j \to Enc'(m_2, m_3) = Enc_k(m_2), Enc_k(m_3)$

Trimit spre criptare de exp: $Enc'(m_0, 0) \to Enc_k(m_0), Enc_k(0)$

m_p ← $Enc'(m_2, 0) \to Enc_k(m_2), Enc_k(0)$

m_k ← Trebuie să decriptez m_p și m_k ca să văd care componentă aparține cărui mesaj.

~~Trimit spre decriptare~~

Ca să îmi dau seama dacă a fost trimis m_i sau m_j -> mă uit la prima componentă să văd dacă $= m_0 \to m_i$ criptat

$= m_2 \to m_j$ criptat.

Nu e CCA sigur

④ $H: \{0,1\}^* \to \{0,1\}^n$ funcție hash. rezistentă la a doua preimagine și rezistentă la coliziuni. Def $H^*: \{0,1\}^* \to \{0,1\}^{n+1}$:

$$H'(x) = \begin{cases} 0 \| x, & \text{dc } x \in \{0,1\}^n \\ 1 \| H(x), & \text{altfel} \end{cases}$$

Este H' rezistentă la prima preimagine? ($\forall x$). Argumentați.

Tot ce trebuie făcut este să găsesc un x pt. care H' nu e rezistentă la prima preimagine.

Rezistentă la prima preimagine adică fiind dat un $H'(x)$ nu se poate determina x.

~~În cazul în ca~~ Luăm $H'(x) = 0 \Rightarrow$ ușor vedem $x = 0 \Rightarrow$

$\to$ nu e rezistentă la prima preimagine.

Coss: Pe ramura 2 $H'(x)$ este rezistentă la prima preimagine deoarece $H(x)$ e rezistentă la coliziuni și a doua preimagine).

⑤ Să ne jucăm cu MAC-uri.

Fie (Mac, Vrfy) un Mac sigur definit peste (K, M, T) unde $M = \{0,1\}^n$ și $T = \{0,1\}^{128}$. Este Mac-ul de mai jos sigur. Argumentați.

$Mac'(k, m) = Mac(k, m \oplus m)$

$Vrfy'(k, m, t) = Vrfy(k, m \oplus m, t)$.

~~Observații~~

Mac sigur $\Leftrightarrow$ nu se poate ghici un mesaj și un tag valid nou care nu a fost trimis deja.

Observăm $m \oplus m = 0$ și putem rescrie:

$Mac'(k, m) = Mac(k, 0)$

$Vrfy'(k, m, t) = Vrfy(k, 0, t)$.

Adică putem trimite orice mesaj deoarece tagul generat va fi mereu cel al lui 0. ($Mac(k, 0)$) care va fi mereu autentificat ($Vrfy(k, 0, t)$). $\Rightarrow$ Nu e MAC sigur

⑥ Alice dorește să își genereze o pereche de chei pt. utilizarea ulterioară a sistemului de criptare ElGamal într-o comunicație criptată cu Bob. Alege $q = 463$ (ordinul grupului) și $g = 11$ (generatorul)

a) Jucați rolul lui Alice. Continuați algoritmul și generați 2 chei: o cheie publică și una privată.

b) Bob dorește să îi transmită lui Alice mesajul clar $m = 19$. Cum procedează?

Despre ElGamal

G - grup finit
$m \xleftarrow{R} G$
$g \xleftarrow{R} G$
$g' = m \cdot g$ rămâne aleator în G.
$P_r[m \cdot g = g'] = \frac{1}{|G|}$
Criptare: $g' = m \cdot g$
Decriptare: $m = g' \cdot g^{-1}$
Algoritm: Se generează (G, q, g), se alege $x \xleftarrow{R} \mathbb{Z}_q$ și se calculează $h = g^x$
Cheia publică: (G, q, g, h)
Cheia privată: (G, q, g, x)
Enc: dată o cheie publică (G, q, g, h) și un mesaj $m \in G$ alege $y \xleftarrow{R} \mathbb{Z}_q$ și întoarce $c = (c_1, c_2) = (g^y, m \cdot h^y)$
Dec: Dată o cheie secretă (G, q, g, x) și un mesaj criptat $c = (c_1, c_2)$, întoarce $m = c_2 \cdot c_1^{-x}$

În problema noastră:

a) $(G, 463, 11)$ $q = 463$, $g = 11$.

(R. Olimid: Atenție când alegeți x a.î. $h = g^x$ să treacă odată peste ordinul grupului altfel inutil).

Aleg un $x = 3$

$h = g^x \Rightarrow h = (11^3) \bmod 463$

$\Rightarrow h = 1331 \bmod 463$

$\Rightarrow h = 405$

Cheia publică: $(G, 463, 11, 405)$

Cheia privată: $(G, 463, 11, 3)$

b) Bob are cheia publică: $(G, 463, 11, 405)$ și vrea să trimită $m = 19$

Aleg $y \xleftarrow{R} \mathbb{Z}_{463}$

~~$y = 3$~~ $y = 2$

$c = (c_1, c_2) = (g^y, m \cdot h^y)$

$c = (121, 19 \cdot 405 \pmod{463})$

$c = (121, 7695 \pmod{463})$ $c = (121, 287)$.

7. Se consideră următorul protocol între Alice și Bob care partajează cheia secretă K_{AB}:

a) Alice alege N_A și îi trimite lui Bob mesajul: ("Alice", N_A);

b) Bob alege N_B și îi trimite lui Alice mesajul: $Enc_{K_{AB}}$("Alice", N_A, N_B)

c) Alice confirmă primirea lui N_B, trimițând lui Bob: $Enc_{K_{AB}}(N_B, N_A)$

a) Presupunem că mesajele lui "Alice", N_A, N_B reprezintă blocuri care se criptează separat folosind ECB. În cazul acesta cum poate un atacator pasiv (care doar observă mesajele trimise de-a lungul protocolului) să joace cu succes rolul lui Alice?

b) Dacă în locul modului ECB se folosește un mod definit: $C_i = Enc_K(M_i) \oplus C_{i-1}, \forall i \geq 1$, protocolul devine sigur la atacul anterior?

a) Deoarece sunt blocuri criptate separat. atacatorul poate interschimba blocurile pentru a obține mesaje noi sau poate retrimite mesaje pe care Alice le-a mai trimis deja.
Adversarul nu poate determina cheia, iar atacul funcționează doar dacă nu se folosește autentificare (MACuri).

b). Da? pentru că blocurile nu mai pot fi rearanjate.

Modelul de pe Moodl

1. Un adversar are la dispoziție un buget de 1.000.000 Eur cu care dorește să achiziționeze hardware capabil să execute 2^{20} criptări AES-128 pe secundă. Un dispozitiv costă 50 Eur.
   a) Câte dispozitive poate achiziționa pt. a le folosi în paralel?
   b) Cât timp necesită determinarea cheii?
   c) Este atacul fezabil?

a) $\frac{1.000.000}{50} = 20.000$ dispozitive hardware

b) un ~~capabil~~ dispozitiv $\rightarrow 2^{20}$ criptări pe secundă
20k dispozitive $\rightarrow 20.000 \cdot 2^{20}$ criptări / secundă
AES-128 $\rightarrow$ criptare pe 128 biți $\rightarrow 2^{128}$ posibile chei.
timp necesar $\frac{2^{128}}{2^{20} \cdot 20000} = \frac{2^{108}}{20000}$ f. f. f. f. f. f. mare

c) Nefezabil. $\rightarrow$ ar dura mai mult decât sistemul solar

2. Se consideră $(Enc_k(m), Dec_k(m))$ un sistem de criptare bloc. Se criptează o secvență de blocuri $m_1 || m_2 || m_3 \ldots$ într-o secvență de blocuri $c_1 || c_2 || \ldots$ astfel:

$$c_i = m_{i-1} \oplus Enc_k(m_i \oplus c_{i-1}), i \geq 1$$, m_0 și c_0 vectori inițializare publici și fiseați.

a) Indicați cum se realizează decriptarea
b) Presupunând că un bloc c_i suferă erori de transmisie, care blocuri de text clar sunt impactate?

a). Decriptare adică trebuie să-l scot pe m_i.

~~Rezolvare: $c_{i+1} = m_i \oplus Enc_k(r)$~~

$m_i = m_{i-1} \oplus c_i \oplus c_{i-1}$

b) Dacă un bloc c_i este afectat atunci mesajele m_i este afectat

Fie $F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ PRF. Se definește un sistem de criptare (Enc, Dec) cu funcția de criptare $Enc_k(m) = r || (F_k(m) \oplus r \oplus 0^n)$ unde r este o valoare aleatoare pe n biți. Arătați că sistemul nu e CCA sigur.

A $\xrightarrow{m_1, m_2,\ |m_1|=|m_2|}$ B $b \in \{0,1\}$ P_B determinist.
$\xleftarrow{c_1, c_2}$

$F_k(m) \oplus r \oplus 0^n$

Trimit $m_1 \| 0$ → ultimul bit e 0

b.

Trimit $m_1 \| 0$ $\xrightarrow{\text{cript}}$ ultimul bit e 0 → ~~decriptez~~
Trimit $m_2 \| 1$ $\xrightarrow{\text{cript}}$ ultimul bit e 1 → ~~decriptez~~
De ce nu e determinist? Ghinion
Defapt nu chiar:

Pot trimite la oracolul de decriptare: $\tilde{0} \| (F_k(m) \oplus r \oplus 0^n)$
și îmi dă criptarea. Scot primi n biți și am criptarea mesajului și compar cu ce aveam inițial (ultimii n biți).

(2a) $\forall i: c_i = m_{i-1} \oplus Enc_k(m_i \oplus c_{i-1})$

$m_{i-1} \oplus c_i = Enc_k(m_i \oplus c_{i-1})$ / Aplic Dec_k

$Dec_k(m_{i-1} \oplus c_i) = m_i \oplus c_{i-1}$ / $\oplus c_{i-1}$

$Dec_k(m_{i-1} \oplus c_i) \oplus c_{i-1} = m_i$.

b) Doar m_i (și evident tot ce urmează după m_i)

(4) $Enc_k(m)$ criptare bloc sigur. H:
i. m se concatenează cu 0-uri până la un multiplu de lungimea blocului
ii. Se sparge secvența obținută în n blocuri: $m_0 \| m_1 \| \dots \| m_{i-1}$
iii. Se aplică:

1. $c \leftarrow Enc_{m_0}(m_0)$.
2. for $i = 1$ to $n-1$ do
3. $d \leftarrow Enc_{m_0}(m_i)$.
4. $c \leftarrow c$ Nor d.
5. end for
6. $H(m) \leftarrow c$.

Este H rezistentă la coliziuni?

Nu deoarece toate blocurile se NORează între ele și pentru orice permutare a blocuri inițiale se obține același rezultat.

Eg: $m_i = m_0 \| m_1 \| m_2$
$m_j = m_1 \| m_0 \| m_2$
$\Rightarrow$ aceeași fct hash deoarece
$c_i = m_0$ NOR m_1 NOR $m_2 = x$
$c_j = c_1$ NOR c_0 NOR $c_2 = y$ $x = y$

⑤ Fie (Mac, Vrfy) un MAC sigur definit peste (K, M, T), unde $M = \{0,1\}^n$ și $T = \{0,1\}^{128}$. Este MAC-ul de mai jos sigur? Arg. răspunsul

$Mac'(K, m) = Mac(K, m \| 0)$.
$Vrfy'(K, m, t) = Vrfy(K, m \| 0, t)$.

Nu este sigur deoarece ultimul bit al lui m este ignorat așadar pt fiecare mesaj de lungime n vor fi alte 2 mesaje care vor genera același tag.

⑥ Fie G un grup de ordin prim q și g un generator al lui G. Considerăm o variantă a schemei de criptare ElGamal în care criptarea unui mesaj $m \in \mathbb{Z}_q$ este aleator. Pt $1 \le m \le B$, arătați cum se poate decripta c cu cheia secretă $x = \log_g h$ folosind o singură exponențiere și $O(B)$ operații pe grup (înmulțiri).

cheia publică: (G, g, h) $c \leftarrow (g^r, g^m h^r)$. $r \xleftarrow{R} \mathbb{Z}_q$
cheia secretă: $x = \log_g h$

$c = (\underbrace{g^r}_{c_1}, \underbrace{g^m h^r}_{c_2})$

$m = \log_g(c_2 \cdot c_1^{-k})$
$m = \log_g(g^m \cdot h^r \cdot g^{-rk})$
$m = \log_g(g^m \cdot g^{\log_g h \cdot r} \cdot g^{-rk})$
$K = -\log_g h \cdot \log_g g$

Verificăm
$m = \log_g(g^m \cdot g^{\log_g h \cdot r} \cdot (g^{-\log_g h \cdot r})^{\log_g g})$
$m = \log_g(g^m \cdot g^{\log_g h \cdot r} \cdot g^{-\log_g h \cdot r}) \cdot \log_g g$
$m = \log_g(g^m) \cdot \log_g g$
$m = \log_g(g^m)$

El gamal ic. cr
Enc $c \leftarrow (g^y, m \cdot h^y)$ x
Dec $m = c_2 \cdot c_1^{-x}$
$h = g^x$
$m \cdot g^{x \cdot y}$
$g^y, m \cdot g^{x \cdot y}$
$g^{m} h^{r} \cdot g^{k}$
$g^m g^{\log_g h \cdot r} \cdot g^{k}$
$g^m h^r \cdot g^k$
$K = -\log_g h \cdot r$
$g^m \cdot g^{-x \cdot r}$
$g^x \cdot \frac{1}{g^x}$
$2^2 \cdot 2^{-2}$
$2^4 \cdot \frac{1}{2^4} = 1$
$\log_2 2^2 = 2$
$g^m \Rightarrow m = \log_g g^m =$
g^m.

$\oplus m_i$ $c_i = m_{i-1} \oplus 00\ldots0 \oplus Enc_k(m_i \oplus c_{i-1})$.

Deci $m_{i-1} \oplus c_i = Enc_k(m_i \oplus c_{i-1})$

$Dec_k(m_{i-1} \oplus c_i) = (m_i \oplus c_{i-1}) \oplus c_{i-1}$

$Dec_k(m_{i-1} \oplus c_i) \oplus c_{i-1} = m_i$.

7. a) Alice alege $k, r \leftarrow \{0,1\}^n$ aleator și îi trimite lui Bob: $s := k \oplus r$

b) Bob alege $t, t \leftarrow \{0,1\}$ aleator și îi trimite lui Alice $u := s \oplus t$

c) Alice calculează $w := v \oplus r$ și îi trimite w lui Bob.

d) Alice întoarce k, iar Bob. calculează $w \oplus t$.

Cerințe:

a) Arătați că Alice și Bob. calculează aceeași cheie.

b) Analizați securitatea schemei (arătați un atac concret dacă există)

a) Alice calculează:

1 $k \oplus r \oplus t \oplus r$ și întoarce k

Bob calculează:

$k \oplus r \oplus t \oplus r \oplus t$ și are cheia k

b). Un atacator care observă mesajele între cei doi vede: $w = k \oplus r \oplus t \oplus r$

Alice 1) $k \oplus r$ $\rightarrow$ $k \oplus r$

2) $k \oplus r \oplus t$ $\rightarrow$ $k \oplus r \oplus t$

3) $k \oplus t$ $\rightarrow$ $k \oplus t$

Ce poate xora pe toate 3 între ele și obține: $k \oplus r \oplus k \oplus r \oplus t \oplus k \oplus t = k$

a obținut cheia iar acum poate trimite ce mesaj vrea dânsul.

Rezolvarea tainelor universului
Part 4

① Se consideră un cod PIN format din 4 cifre (0-9)
a) Câte coduri PIN distincte există?
b) Cât timp necesită determinarea codului PIN dc. se poate efectua o încercare pe secundă?
c) Este atacul fezabil? (dc codul se schimbă odată pe an)

a) a b c d
↓
10 cifre

$10 \cdot 10 \cdot 10 \cdot 10 = 10^4$
a b c d

b) 1 încercare ---- 1 sec
10^4 — — — x

$x = 10^4$ sec

c) 10^4 sec = 10.000 secunde
1 h = 3600 sec
> Timp necesar: maxim 3 h

c) Este fezabil.

② Se consideră modalitatea de Padding OAEP modificată definită ca $OAEP(m,r) = x_1 || x_2$:

$x_1 = m || 1^{n/2} \oplus G(r)$
$x_2 = r \oplus H(x_1)$

$m \in \{0,1\}^{n/2}$, r - val aleat pe n biți, G și H funcții Hash pe n biți.
Indicați cum se calculează m.

$x_1 = m || 1^{n/2} \oplus G(r) \mid \oplus G(r)$
$x_1 \oplus G(r) = m || 1^{n/2}$

Primii n/2 biți ai lui $x_1 \oplus G(r)$ aparțin lui m

③ Fie (Enc, Dec) sistem criptare simetrie. Se consideră sist. criptare (Enc', Dec') pt. mesaje de dim. dublă:

$Enc'_k(m_1 || m_2) = (Enc_k(m_1 \oplus m_2), Enc_k(m_2))$

Arătați că m_n e ECA sigur.

$m_i \begin{bmatrix} m'_1 = 1^n \\ m_2 = 0^n \end{bmatrix} m_j \begin{bmatrix} m_1 = 0^n \\ m_2 = 1^n \end{bmatrix}$ > $(Enc_k(m_2), Enc_k(m_2))$

$(Enc_k(m_1), Enc_k(m_2))$.

A $\xrightarrow{m_1, m_2}$ $\{ b \in \{0,1\}$

Mă uit la prima componentă și la 2a
Dc sunt dif e m_i, dc sunt egale e m_j

④ Se consideră $H: \{0,1\}^* \to \{0,1\}^n$ o funcție hash. rezistentă la a doua preimagine și rezistentă la coliziuni. Se definește o funcție $H^*: \{0,1\}^* \to \{0,1\}^{2n}$:

$$H'(x) = \begin{cases} x \| 1, & x \in \{0,1\}^n \\ H(x) \| 0, & \text{altfel.} \end{cases}$$

Este H' rezistentă la prima preimagine ($\forall x$)? Argumentați

Luăm și noi $H'(x) = 1$ și vedem imediat că $x = 1 \Rightarrow$
$\Rightarrow \exists\ x$ pt. care se poate determina $H'(x)$. $\Rightarrow$ nu e safe

⑤ Fie $(Mac, Vrfy)$ un MAC sigur definit peste (K, M, T), unde $M = \{0,1\}^n$ și $T = \{0,1\}^{128}$. Este MAC-ul de mai jos sigur? Argumentați

$Mac'(k, m) = Mac(k, m)$

$$Vrfy'(k, m, t) = \begin{cases} Vrfy(k, m, t), & \text{dc } m \neq 1^n \\ 1, & \text{altfel} \end{cases}$$

Cred că nu pentru că atacatorul poate autentifica mesajul 1^n oricum.

⑥ El-Gamal

Alice dorește să își genereze o pereche de chei pentru utilizarea ulterioară a sist. de criptare ElGamal într-o comunicație criptată cu Bob. Alege $q = 439$ (ordinul) și $g = 19$ (generatorul)

a) Jucați Rolul lui Alice. Generați cheia publică și privată

b) Bob dorește să transmită lui Alice mesajul clar $m = 4$. Cum procedează

a) $G(439, 19)$

Aleg $x = 3$.

$h = g^x \Rightarrow h = 19^3 = 6859 \bmod 439 \Rightarrow h = 274$

Cheia publică: $(G, 439, 19, 274)$

Cheia privată: $(G, 439, 19, 3)$

b) Aleg $y \xleftarrow{R} \mathbb{Z}_{19}$

$y = 4$

$c = (c_1, c_2) = (g^y, m h^y)$

$c = (19^4, 19 \cdot 274^4)$

$c = (377, 53)$.