تمرین 2 امنیت «به نام خدا» امیرمحمد پیرحسین لو
9531014

---

① joey doesnt share food $k=23$

* (جای سوال دوم اشتباه شده است)

② الف)

$x_1 = P_1 = C_1 \oplus Enc(IV)$

$x_2 = P_2 = C_2 \oplus Enc(C_1)$

$x_3 = P_3 = C_3 \oplus Enc(C_2)$

$\vdots$

$x_i = P_i = C_i \oplus Enc(C_{i-1})$

ب) عملیات رمزگشایی را می‌توان مواردی انجام داد زیرا در مرحله نام تنها به C_i و C_{i-1} احتیاج داریم نه P_k ها.

③

round $i \longrightarrow$ input $= \overline{L_{i-1}}, \overline{R_{i-1}}, \overline{k_i}$ → complement sign

$L_i = R_{i-1} \Longrightarrow \overline{L_i} = \overline{R_{i-1}}$

$\overline{R_i} = \overline{L_{i-1}} \oplus f(\overline{R_{i-1}}, \overline{k_i}) \overset{A}{=} \overline{L_{i-1}} \oplus f(R_{i-1}, k_i) = \overline{L_{i-1} \oplus f(R_{i-1}, k_i)}$

A: $f(\overline{R}, \overline{k}) = f(R, k)$

با ظاهر وجود xor بین k و R

خاصیت xor

$\overline{(101) \oplus (100)} = \overline{110} = \overline{(101 \oplus 100)} = (001)$

⟸ خاصیت مکمل در تمام مراحل اعمال می‌شود و در مرحله آخر عبارت به دست آمده مکمل متن رمزشده در حالت عادی است ⟸ $y_2 = C(y_1)$

preimage resistant : (a) (4)

به ازای هر h یافتن x ای که $H(x)=h$ شود از نظر محاسباتی غیرممکن (سخت) است.

(b) به ازای نمی‌توان جفت (x, y) ای را یافت که $H(x)=H(y)$ شود ← computationally infeasible

(c) به ازای هر بلاک x، یافتن بلاک y که $H(y)=H(x), y \neq x$ غیرممکن (سخت) است.

(a) (5)

2067 → real length = 12 bits

length field : 00...00 1000 0010 1011
t116 t12

padding " : 1 000...0
t1 t876
t877

(b)

2944 : 00...00 1011 1000 0000 ← length field
t116 t12

padding : 1 000...0
t1 t1023

(c)

3000 : 00...00 1011 1011 1000 ← length field
t116 t12

padding field : 1 00...00
t1 t967
t968

---

(6)

$p=17 \quad q=11 \quad pq=187 \quad \phi(pq)=(1-p)(1-q)=160$

$e=7$ (اول نسبت به 160، $7<160$) $\quad de \overset{160}{\equiv} 1 \Longrightarrow d=23$

$PU=\{7,187\} \quad PR=\{23,187\}$

$C=(88)^7 \bmod 187 = 11$

$q = 5 \quad \alpha = 2$

$X_A = 4 \quad X_B = 3$

$\Rightarrow Y_A = \alpha^{X_A} \bmod q = 2^4 \bmod 5 = 1$

$Y_B = \alpha^{X_B} \bmod q = 2^3 \bmod 5 = 3$

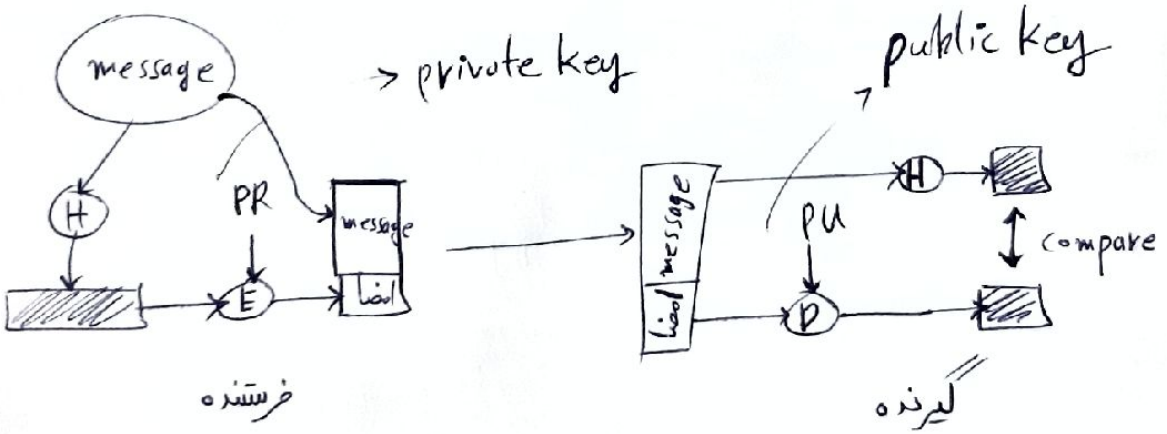
$Y_B^{X_A} \bmod q = 3^4 \bmod 5 = 1$

$Y_A^{X_B} \bmod q = 1^3 \bmod 5 = 1$

$\Rightarrow$ shared secret key $= 1$

---

(8) بلاکی از plaintext که وابسته به آن است انتخاب می شود. (authenticator) این بلاک این ویژگی را دارد که با تغییر plaintext حتما تغییر پیدا می کند. پس این بلاک به وسیله کلید رمزنگاری فرستنده رمز می شود این بلاک رمزشده (امضا) صحت داده و محتوا و مبدا و شماره ترتیب را تأیید می کند. (کلید خصوصی) این فرآیند را می توان توسط HA-1 ای انجام داد. پس این امضا (بلاک رمزشده) به داده متصل می شود و فرستاده می شود.



در این روش داده (message) رمزنگاری نمی شود و قابل مشاهده است. در مواقعی که محرمانه بودن پیام اهمیت چندانی ندارد و سرعت رمزنگاری و استفاده کم از حافظه اهمیت دارد از DSA استفاده می کنیم.