باسمه تعالی

تمرین سری ششم

مبانی رمزنگاری و امنیت شبکه

پوریا دادخواه - ۹۴۱۰۴۳۸۵

دکتر میرحسینی

۱- الف) برای وقوع بیت ۰ در خروجی باید یکی از دو حالت $\begin{cases} P_i=0 \\ K_i=0 \end{cases}$ یا $\begin{cases} P_i=1 \\ K_i=1 \end{cases}$ رخ دهد.

$$\mathbb{P}(P_i=1, K_i=1) = 0.3 \times 0.4 = 0.12$$
$$\mathbb{P}(P_i=0, K_i=0) = 0.7 \times 0.6 = 0.42$$
$$\xrightarrow{+} \mathbb{P}(C_i=0) = 0.54$$

ب) احتمال وقوع صفر در متن اصلی را P و وقوع یک را $1-P$ می‌گیریم. حال احتمال وقوع صفر در متن رمز را مشابه الف بدست می‌آوریم:

$$\mathbb{P}(P_i=0, K_i=0) = P \times \frac{1}{2}$$
$$\mathbb{P}(P_i=1, K_i=1) = (1-P) \times \frac{1}{2} = \frac{1}{2} - \frac{P}{2}$$
$$\xrightarrow{+} \mathbb{P}(C_i=0) = \frac{1}{2} - \frac{P}{2} + \frac{P}{2} = \frac{1}{2} \checkmark$$

پس احتمال $\mathbb{P}(C_i=1) = 1 - \frac{1}{2} = \frac{1}{2}$ ✓ ■

۲- (82) اگر n اول باشد می‌شود دوره تناوب $n-1$ داشت و در این حالت که بایست توان ۲ بدهیم. باید حالات را بررسی کنیم

اگر $a=2k$ یعنی زوج انتخاب شود که دوره تناوب خیلی پایین خواهیم داشت (2 ..)

پس واضح است که برای دوره تناوب بالا باید a فرد باشد، از طرفی می‌دانیم مربع هر عدد فرد به صورت $8k+1$ می‌باشد پس داریم ⇐

$$(2k+1)^4 = (8k'+1)^2 = 16k''+1$$

!

بنابراین برای اعداد فرد هم بیشترین دوره تناوب ممکن $\frac{16}{4}$ است.

b) همانطور که در قسمت قبل گفته شد در درجه اول a حتماً باید فرد باشد

حال از بین اعداد $a = 3, 5, 11, 13$ ، اعداد 7، 9، 15 خوب نیستند و کمترین مناسب خوب است و دوره تناوب 4 (البته به x_0) می‌تواند بدهد.

c) واضح است که اگر x_0 زوج باشد دوره تناوب را کم می‌کند

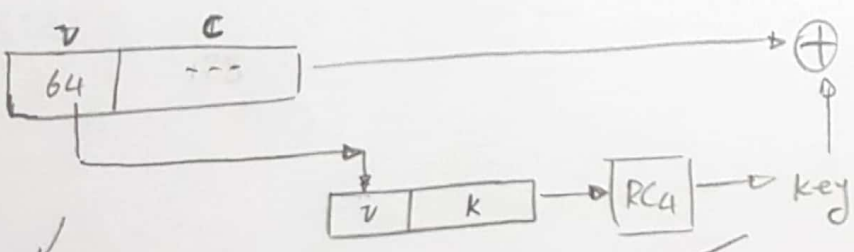
$$a^i x_0 \overset{16}{\equiv} a^j x_0$$

$$x_0 = 2k \quad a^i \overset{8}{\equiv} a^j \quad x \to 0$$ مطلوب ثبت.

ولی همین که x_0 فرد باشد کافی است و شرط خاص دیگری ندارد. ■

۲ـ (8-8)

a) می‌دانیم پیام رمزشده $C \| IV$ است که 64 بیت نخستین v و 128 بیت بعدی C است. پس ابتدا 64 بیت نخست را جدا می‌کنیم و با k ترکیب کرده $(v \| k)$ و درنهایت key را می‌سازیم. حال درنهایت ساخت را شده با C (128 بیت بعدی پیام رمزشده) XOR می‌کنیم.



b) در حالتی که 64 بیت اول پیام فرستاده شده یکسان باشد یعنی $v_2 = v_1$، طرف گیرنده نتیجه می‌گیرد که از جریان کلید تکراری استفاده شده پس روش تست a می‌توان پیام m_1، m_2 را بدست آورد (بدون دانستن k)

c) چون k ثابت است، تنها بخش تغییر در کلید v است. با توجه به مسئله روز تولد برای v، 64 بیتی حدود $\sqrt{\frac{\pi}{2}\times 2^{64}} \simeq 2^{32}$ پیام لازم است فرستاده شود تا v یکسان دیده شود و یک جفت کلید کامل ۲ بار استفاده شده باشد. ■

d) با توجه به نتیجه قسمت قبل، کلید k باید بعد از 2^{32} پیام عوض شود تا مهاجم نتواند پیام را رمزگشایی کند. ■

--- --- --- ---

8.9 (a) چون توزیع بیت‌ها مستقل‌اند داریم:

$$\mathbb{P}(01) = \mathbb{P}(10) = (0.5+\partial)(0.5-\partial) = 0.5^2 - \partial^2 = 0.25 - \partial^2$$

$$\mathbb{P}(00) = (0.5-\partial)^2 \quad , \quad \mathbb{P}(11) = (0.5+\partial)^2$$

b) در دنباله جدید چون فقط از 01 و 10 استفاده شده و احتمال رخداد این دو در دنباله اصلی یکسان است، احتمال وقوع 0 و 1 نیز در خروجی برابر است.

$$\mathbb{P}(0) = \mathbb{P}(1) = 0.5$$

که برای وقوع هر کدام احتمال $0.25 - \partial^2$ در دنباله اصلی باید اتفاق بیفتد.

c) در دنباله‌ی اولیه احتمال وقوع 01 یا 10 برابر $0.5 - 2\partial^2$ است و سایر رشته‌ها حذف می‌شوند یعنی با احتمال گفته شده، هر بیت در دنباله‌ی اولیه مفید است و بقیه دور ریخته می‌شوند. فرض کنیم d طول دنباله اولیه باشد، پس نهایتاً $d\times(0.5-2\partial^2)$ بیت مفید خواهد بود و هر یک از بیت‌ها

در دنباله جدید، از ۲ بیت دنباله اولیه به وجود آمده اند ⇐

$$d(0.5 - 2\partial^2) = 2\chi \rightarrow d = \frac{2\chi}{0.5 - 2\partial^2}$$

d) دنباله خروجی مستقل نخواهد بود، یعنی بیت بعدی به بیت قبلی در خروجی وابسته است.

فرض کنید دنباله ورودی 01011110 باشد. در این صورت دنباله خروجی ۴ صورت 0101 خواهد بود. یعنی مثلاً اگر تعداد زیادی ۱ داشته باشیم در خروجی هم آن را صرفنظر میشود و همیشه پس از یک بیت صفر در خروجی یک بیت ۱ خواهیم داشت پس همیشه بعد از ۱، ۰ و بعد از ۰، ۱ خواهیم داشت.

0101 → 010
0111 → 01
011⋯10 → 010

(9.2)-5

$$\begin{cases} P = 7 \\ q = 17 \end{cases} \quad n = 7 \times 17 = 119 \quad e = 11 \quad \varphi(n) = 6 \times 16 = 96 \quad d = e^{-1} \bmod 96$$

(c

$$\Rightarrow d = 11^{\varphi(n)-1} = 11^{95} \equiv 35$$

$$\Rightarrow \begin{cases} C = M^e \bmod n \Rightarrow C = 11^{11} \bmod (119) = 114 \\ M = C^d \bmod n \Rightarrow M = 114^{35} \bmod (119) = 11 \checkmark \end{cases}$$

ادامه حل بعد

قسمت e)

$$\begin{cases} p = 17 \\ q = 23 \end{cases} \qquad n = 17 \times 23 = 391$$

$$\varphi(n) = 16 \times 22 = 352$$

$$e = 9$$

$$\Rightarrow d = e^{-1} \bmod \varphi(n) = 9^{-1} \bmod 352 \Rightarrow d = 313$$

$$\Rightarrow \begin{cases} C = M^{e} \bmod n \Rightarrow C = 7^{9} \bmod 391 = 61 \\ M = C^{d} \bmod n \Rightarrow M = 61^{313} \bmod 391 = 7 \end{cases}$$

9.7) زمانی که d برای مهاجم مشخص می‌شود با داشتن e و d و n دیگر به دست آوردن φ(n) و یا در واقع تجزیه n به p و q کار مشکلی نیست.

حال اگر با همین n، صرفاً e′ و d′ را تولید کنیم چون مهاجم φ(n) را می‌داند و e′ نیز Public است، d′ به راحتی به دست می‌آید و Bob هر پیامی بنویسد توسط مهاجم شکسته می‌شود. حتی می‌تواند بجای او پیام بنویسد چرا که private آن را دارد.!