بسم الله الرحمن الرحیم

تمرین سوم درس مبانی امنیت شبکه های کامپیوتری

دکتر سعیدی

مهدی وجهی - ۸۱۰۱۰۱۵۵۸

سوال ۱

a

بیت ها مستقل هستند بنابراین قانون ضرب جواب میده.

$$P(00) = P(0)P(0) = (\frac{1}{2} - \delta)(\frac{1}{2} - \delta) = \frac{1}{4} + \delta^2 - \delta$$
$$P(11) = P(1)P(1) = (\frac{1}{2} + \delta)(\frac{1}{2} + \delta) = \frac{1}{4} + \delta^2 + \delta$$
$$P(01) = P(0)P(1) = (\frac{1}{2} - \delta)(\frac{1}{2} + \delta) = \frac{1}{4} - \delta^2$$
$$P(10) = P(1)P(0) = (\frac{1}{2} + \delta)(\frac{1}{2} - \delta) = \frac{1}{4} - \delta^2$$

b

$$P_T = P(01) + P(10) = (\frac{1}{4} - \delta^2) + (\frac{1}{4} - \delta^2) = \frac{1}{2} - 2\delta^2$$
$$P_0 = \frac{\frac{1}{4} - \delta^2}{\frac{1}{2} - 2\delta^2} = \frac{1}{2}$$
$$P_1 = \frac{\frac{1}{4} - \delta^2}{\frac{1}{2} - 2\delta^2} = \frac{1}{2}$$

c

احتمال تولید هر بیت خروجی به ازای بیت ورودی را حساب می کنیم.

$$0 \times P(00) + 0 \times P(11) + \frac{1}{2} \times P(10) + \frac{1}{2} \times P(01) = \frac{1}{4} - \delta^2$$

بنابراین نرخ تولید می شود:

$$\frac{x}{\frac{1}{4} - \delta^2}$$

سوال ۲

خیر ناامن است. یک راه ساده تحلیل آماری بسیار ساده روی داده رمز شده است و به آسانی با فرکانس داده ها و حروف پرتکرار نگاشت موجود را پیدا می کنیم و داده ها را تبدیل می کنیم. راه دیگر هم این است که چون n, e مشخص است و فضای موجود محدود می توانیم ۲۶ نگاشت را پیدا کنیم و از این نگاشت استفاده کنیم.

سوال ۳

حل با روش آزمایش جواب ها

با یک کد ساده پایتون به شکل زیر مسئله را حل می کنیم.

```
n = [[1,3],[2,2],[3,5],[4,6],[5,1],[6,4]]

hist = [[] for i in range(len(n))]
for i in range(10000):
    for j in range(len(n)):
        if i == n[j][0]:
            n[j][0]+=n[j][1]
            hist[j].append(n[j][0])
    count = 0
    for j in range(len(n)):
        if n[j][0] == n[0][0] and n[j][0] % 7 == 0:
            count += 1
    if count == len(n):
        print(n[0][0])
        # for j in hist: print(j, '\n\n')
        break
```

جواب هم میشه ۲۳۸ تمین روز.

حل با روش باقی مانده های چینی

محدودیت های مسئله را می نویسیم.

محدودیت	محدود کننده
$x = 1 \, mod 3$	استاد ۱
$x = 2 \, mod 2$	استاد ۲
$x = 3 \, mod 5$	استاد ۳
$x = 4 \, mod 6$	استاد ۴
$x = 5 \, mod 1$	استاد ۵
$x = 6 \, mod 4$	استاد ۶
$x = 0 \, mod 7$	دانشگاه

برای این که مسئله مدل شده را با باقی مانده چینی حل کنیم باید باقی مانده ها نسبت به هم اول باشند پس لازم است مواردی که این شرط را ندارد تجمیع کنیم.

$x = 4\ mod6 \Rightarrow x = 0\ mod2,\ x = 1\ mod3$

پس شروط ۱ و ۲ و ۴ در شرط ۴ جمع میشه.

شروط زیر نسبت به هم اول نیستند پس در یک شرط تجمیع می کنیم.

$x = 6\ mod4, x = 4\ mod6 \Rightarrow\ x = 10\ mod12$

همچنین شرط زیر بدیهی است و حذف می شود:

$x = 5\ mod1$

در نهایت با اشتراک گیری و ساده سازی و حذف موارد بدیهی شرایط به شکل زیر است.

$x = 10\ mod12$
$x = 3\ mod5$
$x = 0\ mod7$

حال در فرمول قرار می دهیم و حل می کنیم.

$M = 12 \times 5 \times 7 = 420$

$x = 10 \times \frac{420}{12} \times (\frac{420}{12})_{12}^{-1} + 3 \times \frac{420}{5} \times (\frac{420}{5})_{5}^{-1} + 0 \times \frac{420}{7} \times (\frac{420}{7})_{7}^{-1} = 10 \times 35 \times 11 + 3 \times 84 \times 4$
$= 4858 \Rightarrow 4858\ mod420 = 238$

سوال ۴

ابتدا به صورت شفاف سر a, q توافق می کنند مانند الگوریتم اصلی سپس گام های زیر طی می شود.

هر دو کلید عمومی Y_A, Y_B و نانس ها N_A, N_B را حساب می کنند. سپس A بسته زیر را تشکیل می دهد و ارسال می کند:

$E(PR_A, Y_A||N_A)$

دلیل رمز کردن با کلید خصوصی این است که احراز شود این پیام توسط A ارسال شده و کس دیگری مانند مرد میانی نیست و بسته ای با کلید خصوصی A بسازد. برای رفع مشکل بازپخش پیام نانس تصادفی قرار دادیم بنابراین اگر این پیام مجدد دریافت شود B متوجه می شود که این نانس تکراری است و مورد حمله قرار گرفته. تنها مشکلی که وجود دارد این است که این نانس باید ذخیره شود و دیگر استفاده نشود، این موضوع در طول زمان می تواند سخت و مشکل ساز باشد. برای حل این مشکل ما می توانیم این نانس ها را در زمان کوتاهی نگه داریم مثلا ۱ دقیقه و به پیام خود برچسب زمانی اضافه کنیم. با این کار پیام هایی که در بازه زمانی مجاز قرار دارند با نانس های قبلی (موجود در بازه زمانی معتبر) مقایسه می شود و اگر تکراری نبود پذیرفته می شود و در اگر تکراری بود حمله تلقی می شود. اگر خارج از بازه مجاز بود دیگر نانس بررسی نمی شود و حمله تلقی می شود. این موضوع مشکل قبلی را حل می کند و دیگر نیاز به ذخیره طولانی مدت نانس ها نیست و حمله بازپخش دفع می شود. در نهایت بسته ارسالی اول از A به B به شکل زیر است:

$E(PR_A, Y_A||N_A||TimeStamp)$

با دریافت این پیام B از این که پیام توسط A است و تغییر نکرده و همچنین عدم بازپخش مطمئن می شود. همچنین B نیز پیام مشابهی تولید می کند و برای A می فرستد. که به شکل زیر است:

$E(PR_B, Y_B||N_B||TimeStamp)$

با دریافت این پیام A از این که پیام توسط B است و تغییر نکرده و همچنین عدم بازپخش مطمئن می شود. با توجه به این که دو طرف همدیگر را احراز کرده اند و حملات گفته شده هم دفع شده، می توانند با خیال راحت کلید نشست خود را بسازند و ارتباط امن را برقرار کنند.

سوال ۵

این باعث می شود که دیگر مسئله برای حل نیاز به لگاریتم گسسته نداشته باشد که سخت است و بتوان با لگاریتم معمولی (تقسیم پی در پی) جواب مسئله را پیدا کرد. عدد کوچک تر را انتخاب می کنیم و بر پایه ۳ تقسیم می کنیم ۲۷ ، ۹، ۳، ۱ یعنی ۳ به توان ۳ یعنی می توانیم کلید عمومی دوم را را به توان ۳ برسانیم تا کلید نشست به دست بیایید. یعنی ۲۴۳ به توان ۳ که معادل ۱۴۳۴۸۹۰۷.

منابع

https://gemini.google.com/share/0950203623dc
https://gemini.google.com/share/5a53d05a5947
https://gemini.google.com/share/e5af5bc3c54a
https://chatgpt.com/share/69143e12-c208-8001-a011-f941058c910a
https://chat.qwen.ai/s/4f1b0b67-853b-4a49-87cd-4a04a0323966?fev=0.0.243
https://claude.ai/share/0c1a3dfd-84d8-4dc0-b467-05a4c3ebb1e8
https://gemini.google.com/share/e3f46813b4c1
https://chatgpt.com/share/69143e12-c208-8001-a011-f941058c910a
https://chat.deepseek.com/share/pfrze86jqkbnpy529z