۱- مزایا و معایب "one-time pad" را بیان کنید.

۲- می‌دانیم که LFSR ها به سه دسته زیر تقسیم می‌شوند:

- Primitive Polynomial
- Irreducible Polynomial
- Reducible Polynomial

۲-۱- تفاوت این سه دسته را بیان کنید.

۲-۲- LFSR های متناظر با چند جمله‌ای های زیر را رسم کرده و مشخص کنید هر یک متعلق به کدام دسته می‌باشند.

$$x^4 + x^3 + x^2 + x + 1$$

$$x^3 + x + 1$$

۳- می‌خواهیم یک حمله ساده بر روی یک رمز جریانی (stream cipher) مبتنی بر LFSR انجام دهیم. یک جفت plain text / cipher text به صورت زیر در اختیار داریم:

Plain text: 1001 0010 0110 1101 1001 0010 0110

Cipher text: 1011 1100 0011 0001 0010 1011 0001

۳-۱- درجه LFSR تولیدکننده‌ی جریان کلید (key stream) چند است؟

۳-۲- مقدار اولیه LFSR را بدست آورید.

۳-۳- ضرایب فیدبک LFSR را تعیین کنید.

۳-۴- با رسم بلوک دیاگرام LFSR ، درستی نتایج بدست آمده را نشان دهید.

۴- برای بررسی اثر بهمنی (Avalanche effect) در رمز DES ، یک ورودی را در نظر بگیرید که فقط بیت ۵۷ ام آن '1' و سایر بیت‌های آن '0' است؛ تمامی بیت‌های کلید نیز '0' است.

۴-۱- چند S-box ورودی‌های متفاوتی در مقایسه با حالتی که تمامی بیت‌های plaintext صفر است، دریافت می‌کنند؟

۴-۲- خروجی پس از دور اول (Round 1) چیست؟

۴-۳- حداقل تعداد بیت‌های خروجی S-box ها که با توجه به طراحی S-box ها تغییر می‌کنند، چقدر است؟

۴-۴- چند بیت خروجی بعد از دور اول در مقایسه با حالتی که تمامی بیت‌های plain text صفر است، تغییر کرده‌است؟

۵- رمز DES دارای کلیدهای weak و semi weak است که به صورت زیر تعریف می‌شوند:

- Weak key: $E_k(E_k(x)) = x$
- Semi weak key: $E_{k_1}\left(E_{k_2}(x)\right) = x$

۵-۱- رابطه‌ی بین sub-key ها در الگوریتم رمزنگاری و رمزگشایی برای برقراری معادله weak key را توضیح دهید.

۵-۲- رمز DES دارای ۴ کلید ۶۴ بیتی weak است. آن‌ها را بیابید.

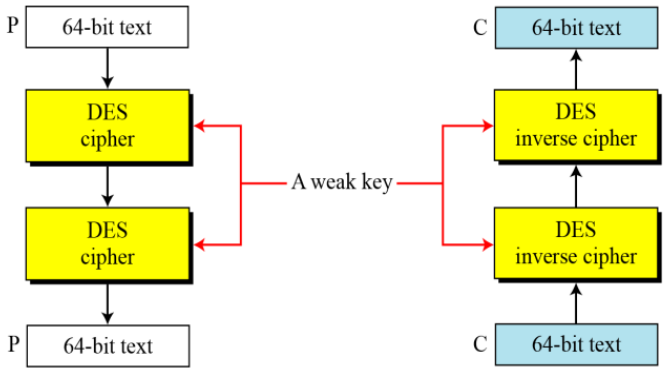
۵-۳- اگر یک کلید به صورت تصادفی انتخاب شود، احتمال این‌که یک کلید weak باشد چقدر است؟

۵-۴- در چه مواقعی نباید از کلیدهای weak استفاده کنیم؟ توضیح دهید.

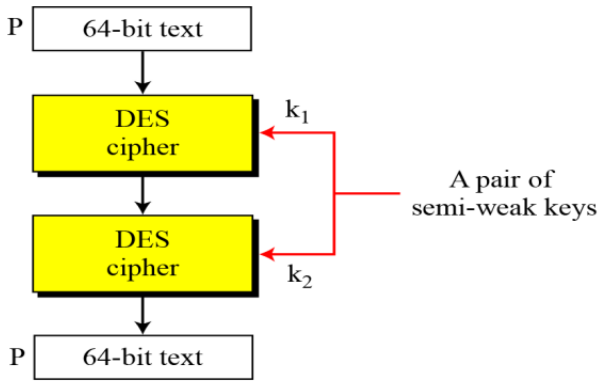
۵-۵- چند جفت کلید semi weak در رمز DES وجود دارد؟

۵-۶- کلیدهای semi weak فقط دو sub-key متفاوت تولید می‌کنند. هر sub-key چند بار در الگوریتم استفاده شده است؟

۵-۷- احتمال انتخاب کلید weak ، semi weak یا possible weak key چقدر است؟



Double encryption and decryption with a weak key



A pair of semi-weak keys in encryption and decryption

سوال اختیاری

۶- به کمک گام‌های زیر نشان دهید:

$$y = DES_k(x) \Rightarrow y' = DES_{k'}(x')$$

۶-۱- نشان دهید به ازای هر رشته بیت A و B با طول یکسان، روابط زیر بر قرار هستند:

$$A' \oplus B' = A \oplus B$$

$$A' \oplus B = (A \oplus B)'$$

۶-۲- نشان دهید : $PC-1(k') = \left(PC-1(k)\right)'$

۶-۳- نشان دهید : $LS_i(C'_{i-1}) = \left(LS_i(C_{i-1})\right)'$

۶-۴- با استفاده از نتایج بالا نشان دهید، اگر $i = 1,2,\dots,16$; k_i کلیدهای ساخته شده از کلید k باشند، آنگاه $i = 1,2,\dots,16$; k'_i کلیدهای ساخته شده از کلید k' هستند.

۶-۵- نشان دهید : $IP(x') = (IP(x))'$

۶-۶- نشان دهید : $E(R'_i) = (E(R_i))$

۶-۷- با استفاده از نتایج بدست آمده نشان دهید، اگر k_i , L_{i-1} , R_{i-1} ؛ R_i را می‌سازند، آنگاه $k'_i , L'_{i-1} , R'_{i-1}$ ؛ R'_i را تشکیل می‌دهند.

۶-۸- نشان دهید : $y = DES_k(x) \Rightarrow y' = DES_{k'}(x')$

تمرین کریپتول:

7- Search about one of the below topics of your choice and write a text with at least 500 words about this topic.

- Differences between stream and block ciphers
- PRESENT block cipher
- Brute-force attack

Note: Answer the below questions making use of CrypTool; use the ECB mode for all the exercises related to the DES algorithm.

7- 1. Search about weak keys of DES and answer the following questions:

i. Encrypt your text twice, with DES algorithm using one of the weak keys for both rounds.

ii. Again, encrypt the text twice, using a DES semi-weak key pair.

7-2. A more secure alternative to DES is Triple DES, answer the following questions surrounding this algorithm:

i. Why is it more secure compared to DES?
ii. When implementing a brute-force attack, how large is its key space? Why is it that long?
iii. Compare its two versions with each other.
iv. Encrypt your text using the CrypTool Triple DES encryption scheme with your desired key.
v. Knowing that CrypTool uses the second version of 3DES, and encrypts the text with k1= k3 (it uses the key of the first encryption round for both the first and the third rounds), Encrypt the same text 3 times using the simple DES algorithm, with k1 = the first half of your key in the previous part, and k2 = its second half.
vi. Try to Decrypt the last output of the previous part using the Triple DES decryption and the same key as in part “iv”.