Understanding Cryptography
Answers of Homework No.3

Chapter 5

1.
1.1. Compare five modes of operation designed to be used with modern Block Ciphers.

حل:

Operation Mode	Description	Data Unit Size
ECB	Each n-bit block is encrypted independently with the same cipher key	n
CBC	Same as ECB, but each block is first exclusive-ored with the pervious cipher text.	n
CFB	Each r-bit block is exclusive –ored with an r-bit key, which is part of pervious text	$r \leq n$
OFB	Same as CFB, but the shift register is updated by the pervious r-bit key	$r \leq n$
CTR	Same as OFB, but a counter is used instead of a shift register.	n

1.2. What are the advantages and disadvantages of Mode ECB?

حل:

مزایا

- به بلوک همزمان‌سازی بین فرستنده و گیرنده نیازی نیست.
- خطاهای بیت ناشی از نویز موجود در کانال فقط بر بلوک مربوط اثر می‌گذارد و بر بلوک های دیگر و قبلی اثری نمی گذارند.
- عملیات رمزنگاری بلوک می تواند به صورت موازی انجام شود.
- سرعت بالای پیاده سازی

معایب

- به ازای هر متن اصلی مشخص متن رمزشده مشخصی نتیجه می‌شود.

- اگر پیام های یکسان دوبار فرستاده شوند مهاجم شناسایی می شود.
- بلوک های متن اصلی به طور مجزا و مستقل از بلوک های قبلی رمز می‌شود.
- مهاجم ممکن است بلوک های متن رمزشده را که منجر به متن اصلی صحیح می شود تغییر دهد.

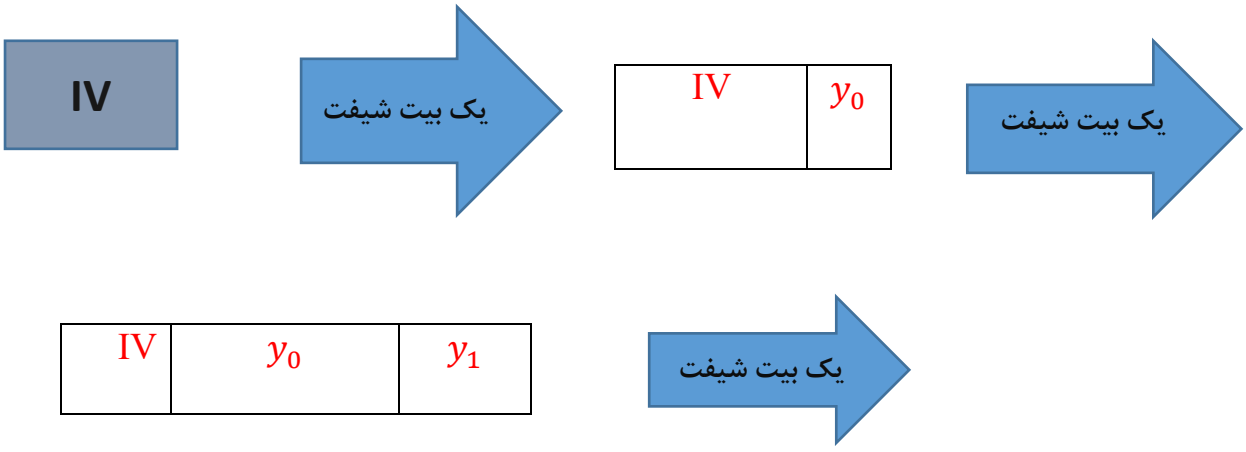
2. Besides simple bit errors, the deletion or insertion of a bit yields even more severe effects since the synchronization of blocks is disrupted. In most cases, the decryption of subsequent blocks will be incorrect. A special case is the CFB mode with a feedback width of 1 bit. Show that the synchronization is automatically re-stored after K + 1 steps, where K is the block size of the block cipher.

حل:

ابتدا از مقدار IV شروع نموده و پس از هر دور با در نظر گرفتن یک بیت فیدبک، فیدبک رجیستر را شیفت می دهیم و بیت جدید را در مکانی ذخیره می‌کنیم. باید توجه داشته باشیم که در یک زمان در هر بار تکرار، یک بیت از متن اصلی رمز می گردد و ۱۲۸ بیت متن اصلی رمز نمی‌گردد. پس خطای همزمانسازی رخ خواهد داد. برای اینکه یک بیت فیدبک به ثبات وارد گردد κ گام داریم. و گام بعدی این خارج از رجیستر انجام می‌شود. اگر یک دنباله بیت شبیه $[\ldots 01011\ldots]$ داشته باشیم یک بیت آن حذف گردد مثلا بیت 0 میانی آن حذف شود این را داریم $[\ldots 0111..]$. این مرحله تا پایان کار ادامه پیدا می کند.

به محض اینکه ثبات به مقدار کافی شیفت پیدا کرد تا شامل $[\ldots 11]$ گردد. مقدار موجود در شیفت رجیستر معادل با چیزی است که حذف شده است. به خاطره این موضوع هم متن اصلی و هم متن رمزشده دارای یک بیت حذف شده می باشند. بعد از $\kappa + 1$گام ، دنباله نادرست در پایان رجیستر از بین می رود.

در واقع در مود CFB زمانی که یک بیت فیدبک می خورد، هر بار IV یک بیت به سمت چپ شیفت می‌یابد و یک بیت در سمت راست قرار می گیرد.



این شیفت ها ادامه دارد. با توجه به اینکه طول بلاک ما K بیت است اگر در بلاکی یک بیت y_i گم یا حذف شود بعد از $k+1$ دور y_i از رجیستر خارج می‌گردد و ادامه رمزگشایی به صورت صحیح خواهد بود.

3.

- Programming

  Complete the file “operationModes.ipynb” related to the implementations of operational modes including ECB, CBC, OFB, CFB, and CTR. In this file, we use AES as our block cipher. For the sake of your convenience, the input string and outputs of functions are processed to make them suitable and compatible for use with the block cipher. This way, all you have to do is to complete the parts in which you’re asked to write your codes. However, feel free to change any parts you deem inconsistent with your needs. At the same time, note that the purpose of this exercise is to have you understand and implement the algorithms yourself. Therefore, using built-in implementations of encryption modes does not merit any score. (To open the file you might need to use ipython or jupyter notebooks)

حل:

در فایل پیوست آمده است.

Chapter 6

Euler’s Phi Function

4. If *p* is a prime and *a* is a positive integer, prove

$$\emptyset\,(p^a) = p^a - p^{a-1}$$

حل:

هدف ما محاسبه تعداد اعداد صحیح نامنفی کوچکتر از $n = p^a$ است که نسبت به n اول هستند.

بهتر است تعداد اعدادی که نسبت به n اول نیستند را محاسبه کنیم و سپس از مقدارکل کم کنیم.

اعداد صحیح نامنفی کوچکتر از p^a عبارتند از $0,1,2,\dots p^a-1$ که تعداد آنها p^a عدد است. اعدادی که یک عامل مشترک با p^a دارند مضارب p هستند مثل : $0, p, 2p, \dots$

پس تعداد $p^a/p = p^{a-1}$ عدد داریم:

$$\emptyset\,(p^a) = p^a - p^{a-1}$$

Wilson theorem

5. If *p* is a prime, prove that

$$\binom{p-1}{k} \equiv (-1)^k \,(mod\ p).$$

حل :

طبق تعریف ضرایب دوجمله ای داریم:

$$\binom{p-1}{k} = \frac{(p-1)!}{k!\,(p-k-1)!} = \frac{(p-1)(p-2)\ldots.(p-k-1)!}{k!\,(p-k-1)!} \qquad mod\ p$$

$$\left(\frac{p-1}{1}\ mod\ p\right) \times \left(\frac{p-2}{2}\ mod\ p\right) \times \ldots. \times \left(\frac{p-(k-1)}{k-1}\ mod\ p\right) \times \left(\frac{p-k}{k}\ mod\ p\right)$$

$$\left(\frac{-1}{1}\right) \times \left(\frac{-2}{2}\right) \times \left(\frac{-k+1}{k-1}\right) \times \ldots. \times \left(\frac{-k}{k}\right)\ mod\ p$$

$$\frac{(-1) \times (-1) \times \ldots. \times (-1)}{k} = (-1)^k \quad mod\ p$$

6. If p is a prime, prove that

$$(p-1)! + 1 = 0\ \ mod\ p.$$

حل :

با توجه به اینکه p یک عدد $prime$ است، اگر $k \in \{1, \ldots., p-1\}$ باشد، در نتیجه k نسبت به p اول است. پس اعداد صحیحی مانند a و b وجود دارند به طوریکه

$$ak + bp = 1 \qquad or \qquad ak = 1 \quad (mod\ p)$$

با کاهش $a\ \ mod\ p$، فرض می شود $a \in \{0, \ldots, p-1\}$ است.

پس، هر المان از مجموعه $\{1, \ldots., p-1\}$ یک پیمانه p متقابل در خود مجموعه دارد. این پیمانه به این صورت کار می کند که المان های $2, \ldots. p-2$ باید به صورت زوج های $\{x, x^{-1}\}$ جفت شوند. و ضرب آن ها یک می شود. پس داریم:

$$(p-1)! = 1.2 \ldots (p-2).(p-1) = 1\,.\,1.(p-1) = p-1 = -1\ (mod\ p).$$

Number Theory

7. Prove that any positive integer of the form $3k+1$ is the form $6k+1$.

8. Prove for n a natural number, If $n \geq 2$ then $n^3 - n$ is always divisible by 3.

حل:

7.

تنها عدد اول زوج ۲ است که این عدد به فرم $3k+1$ نیست. بنابراین هر عدد اول به فرم $3k+1$ فرد است. این یعنی $3k$ باید زوج باشد و درنتیجه k باید زوج باشد $k = 2m$. پس یک عدد اول به فرم $3k+1$ به صورت $3(2m) = 1 = 6m+1$ هست.

8.

اگر یک عدد با ۳ قابل تقسیم باشد می‌تواند به صورت $3r$ به ازای r صحیح نوشته شود.

گام اول:

برای $n = 2$ داریم $2^3 - 2 = 6$ که ۶ توسط ۳ قابل تقسیم است.

گام دوم (فرض استقرا):

فرض می‌کنیم که برای $n = k$ صحیح است. $k^3 - k = 3r$. حال برای $n = k + 1$ اثبات می‌کنیم (حکم استقرا):

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - (k+1)$$
$$= (k^3 - k) + 3k^2 + 3k$$
$$3r + 3k^2 + 3k$$
$$3(r + k^2 + k)$$

در نتیجه اثبات شد. به طور کلی اصل استقرا دلالت بر این دارد که $n^3 - n$ برای $n \geq 2$ توسط ۳ قابل تقسیم است.