سارا برادران

۹۶۲۴۱۹۳

تکلیف سری چهارم رمزنگاری

## Question 1)

1.1

| Operation mode | Description | Type of result | Data unit size |
|---|---|---|---|
| ECB | بلوک های n بیتی به شکل مستقل از هم و جداگانه رمز می شود | N بیت داده ورودی در قالب یک بلوک با کلید k رمز شده و یک قالب رمز N بیتی ایجاد می شود | نیازی به ذخیره سازی نیست زیرا بلوک ها جداگانه رمز می شوند. |
| CBC | بلوک های n بیتی وابسته به هم رمز می شوند به این نحو که iV با بلوک اول متن اصلی xor و سپس رمز می شود و بلوک اول cipher را تولید میکند مجددا در هر مرحله بلوک i-1 ام cipher با بلوک i ام متن اصلی xor و سپس رمز شده و بلوک i ام cipher را تولید می کند. | N بیت داده ورودی ابتدا با iv یا متن رمز شده بلوک قبل در قالب یک بلوک با کلید k رمز شده و یک قالب رمز شده N بیتی ایجاد می شود | به اندازه ورودی یک بلوک رمز قالبی به فضای دخیره سازی نیاز مندیم n |
| CFB | بلوک های n بیتی وابسته به هم رمز می شوند به این نحو که ابتدا IV رمز شده $s_1$ را تولید می کند سپس $s_1$ با بلوک اول متن اصلی xor می شود و بلوک اول cipher را تولید می کند مجددا در هر مرحله بلوک i-1 ام cipher رمز شده و حاصل یعنی si با بلوک i ام متن اصلی xor شده بلوک i ام cipher را تولید می کند. | از حاصل رمز IV یا متن رمز شده بلوک قبل یک رشته بیت تولید می شود که بیت با بیت با متن اصلی xor می گردد. (دارای تابعی مشابه LFSR برای تولید رشته بیت) | به r بیت از متن رمز شده مرحله قبل نیازمندیم r<=n |
| OFB | بلوک های n بیتی وابسته به هم رمز می شوند به این نحو که ابتدا IV رمز شده $s_1$ را تولید می کند سپس $s_1$ با بلوک اول متن اصلی xor می شود و بلوک اول cipher را تولید می کند مجددا در هر مرحله si-1 رمز شده و حاصل یعنی si با بلوک i ام متن اصلی xor شده بلوک i ام cipher را تولید می کند. | از حاصل رمز IV یا دنباله تولید شده بلوک قبل یک رشته بیت تولید می شود که بیت به بیت با متن اصلی xor می گردد. (دارای تابعی مشابه LFSR برای تولید رشته بیت) | به r بیت از خروجی رمز قالبی(s) مرحله قبل نیازمندیم r<=n |
| CTR | بلوک های K بیتی به شکل جداگانه رمز می شوند ولی با تفاوت نسبت به مد ECB بدین نحو که ابتدا ۹۶ بیت IV و ۳۲ بیت شمارنده ای که از صفر آغاز می شود با هم کانکت و سپس رمزشده و با بلوک اول متن اصلی xor شده بلوک اول cipher را تولید می کنند مجددا یک واحد به شمارنده اضافه شده و به همین روش بلوک های بعدیcipher تولید می شوند. | ترکیبی از IV و شمارنده رمز شده و یک رشته بیت تولید می شود که با متن اصلی بیت به بیت xor می گردد. (دارای تابعی مشابه LFSR برای تولید رشته بیت) | به اندازه یک شمارنده فضای ذخیره سازی نیاز مندیم r<=n |

1.2

ECB mode

در این روش ، رمزگذاری هر بلاک مجزا انجام می شود و بلاک های رمز شده به هم وابسته نیستند مثلا دررمز نگاری AES متن plaintext به بلاک های ۱۲۸ بیتی تقسیم شده و هر بلاک جداگانه رمز می شود

### Advantages

به دلیل عدم وابستگی میان بلاک های رمز شده اگر نویز رخ دهد و به هر دلیلی بیت های متن رمز شده دچار خطا شود صرفا این خطا منجر به تولید plaintext اشتباه برای همان بلاک می شود(به طور میانگین اگر یک بیت ciphertext دچار خطا شوند نیمی از بیت های plaintext (۶۴ بیت) دچار خطا می شود.) به علاوه به سبب عدم وابستگی این بلاک ها امکان رمز گذاری بلاک ها به صورت موازی و همزمان وجود دارد که می تواند باعث کاهش زمان صرف شده و سرعت بیشتر رمز گذاری شود.

### Disadvantages

از آنجایی که بلاک ها مجزا هستند لذا بلاک هایی با plaintext مشابه منجر به تولیدciphertext های مشابه می شوندو این از جمله مواردی است که آسیب پذیری را بالامی برد و حملات راامکان پذیر می سازد.مثلا اگر متن اصلی سراسر 0 یا سراسر 1 باشد تمام بلاک ها ciphertext های یکسان تولید می کند.

**Question 2)**

کافی است ابتدا متن رمز شده را با کلیدی که می دانیم به وسیله روش AES-128 رمزگشایی کنیم حاصل بدست آمده ۸ بیت متن خواهد بود که حاصل xor متن اصلی( 0xFF ) با IV می باشد لذا واضح است :

متن رمز شده = (متن اصلی Xor بردار اولیه) $AES\ Encryption_k$

متن اصلی معلوم

متن رمز شده معلوم

بردار اولیه مجهول

**بردار اولیه = متن اصلی xor (متن رمز شده)$_k$ AES Decryption**

به این ترتیب می توان IV را از روی رابطه فوق محاسبه کرده و حال با داشتن کلید و بردار اولیه می توان به سادگی متن رمز شده ثانویه را شکست به این صورت که ابتدا الگوریتم رمز گشایی AES-128 را بر روی آن پیاده کرده سپس نتیجه را با بردار اولیه Xor می کنیم بدین ترتیب متن اصلی ثانویه بدست خواهد آمد.

**Question 3)**

اگر y یک رجیستر k بیتی باشد و یک بیت اشتباه وارد آن شود در مرحله اول به عنوان بیت اول رجیستر قرار می گیرد آن گاه در مرحله دوم ضمن یک واحد شیفت پیدا کردن y ، بیت مذکور به عنوان بیت دوم رجیستر ظاهر می شود و ... به این

ترتیب در K امین مرحله به عنوان بیت k ام رجیستر y ظاهر می شود و از آنجایی که رجیستر K بیتی است ضمن شیفت بعدی یعنی در مرحله K+1 ام از رجیستر خارج می شود و محتوای رجیستر فاقد آن می گردد.

**Question 5)**

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

We know $\varphi(n) = n (1-1/p_1) (1-1/p_2) \dots$ ($p_i$ -> factors of n)

$N = p^a$ and p is a prime number and the only factor of n →

$\varphi(n) = p^a (1 - 1/p) = p^a ((p-1) / p) = (p^{a+1} - p^a) / p = p^a - p^{a-1}$

**Question 6)**

$\binom{p-1}{k} = ( -1 )^k \bmod p$

$$\binom{p-1}{k} = \frac{(p-1)!}{k! * (p-1-k)!} mod\ p = \frac{(p-1)(p-2)\dots(p-k)}{k!}\ mod\ p = \frac{1}{k!} * \big((p-1)(p-2)\dots(p-k)\big) mod\ p = \frac{1}{k!} \bmod p * (p-1\ mod\ p)(p-2\ mod\ p)\dots(p-k\ mod\ p) = \left(\frac{1}{k!} * (-1)(-2)\dots(-k)\ mod\ p\right) = \frac{k!}{k!} * (-1)^k mod\ p = (-1)^k mod\ p$$

**Question 7)**

عدد $6k + 5$ یک عدد فرد است زیرا $6k$ همواره زوج و 5 فرد است و حاصل جمع یک عدد فرد و یک عدد زوج عددی فرد خواهد بود. به علاوه $6k + 5$ بر ۳ بخشپذیر نیست. پس عدد $6k + 5$ نمیتواند عوامل اولی به شکل $6k, 6k + 2, 6k + 3,$ or $6k + 4$ داشته باشد و صرفا عوامل اول آن می توانند به شکل $6k + 1$ یا $6k + 5$ باشند.

اگر عدد $6k + 5$ ضرفا متشکل از عوامل اول به فرم $6k + 1$ باشد خواهیم داشت:

$(6k + 1) * (6k + 1) = 36k^2 + 6k + 6k + 1 = 6(6k^2 + 2k) + 1 = 6k' + 1$

واضح است فرم حاصلضرب هر تعداد عدد به فرم $6k + 1$ در هم نیز $6k + 1$ خواهد بود. پس عدد $6k + 5$ نمیتواند صرفا متشکل از اعداد اول به فرم $6k + 1$ باشد پس دو حالت دیگر باقی می ماند:

۱- عدد $6k + 5$ مشکل از اعداد اول به هردو فرم $6k + 1$ و $6k + 5$ باشد:

$(6k + 1) * (6k + 5) = 36k^2 + 6k + 30k + 5 = 6(6k^2 + 6k) + 5 = 6k' + 5$

این حالت صحیح و پذیرفته است.

۲- عدد $6k + 5$ صرفا متشکل از اعداد اول به فرم $6k + 5$ باشد:

$(6k + 5) * (6k + 5) = 36k^2 + 30k + 30k + 25 = 6(6k^2 + 10k + 3) + 7$

این حالت پذیرفته نیست.

**اعداد مثبت به فرم $6k + 5$ حتما عوامل اول به فرم $6k + 1$ و $6k + 5$ دارند.**

**Question 8)**

$3 \mid n^3 - n$ , for $n >= 2$;

$n^3 - n = n(n^2 - 1) = n(n-1)(n+1) = (n-1) * n * (n+1)$ , $n >= 2 \rightarrow n-1 >= 1$

**مقدار عبارت برابر با حاصل ضرب سه عدد طبیعی متوالی است.**
**(کوچکترین عدد از میان این سه عدد حداقل برابر ۱ خواهد بود)**

**از میان سه عدد طبیعی متوالی حتما یکی از آن ها بر ۳ بخشپذیر است پس حاصلضرب سه عدد طبیعی متوالی نیز همواره بر ۳ بخشپذیر خواهد بود.**

به کمک استقرا نیز می توان این مسئله را اثبات کرد:

پایه استقرا $n^3 - n$ , $n = 2 \rightarrow 8 - 2 = 6$ , $3 \mid 6$ ok

فرض استرا $n^3 - n$ , $n = k \rightarrow 3 \mid k^3 - k$

حکم استقرا $n^3 - n$ , $n = k + 1 \rightarrow ?\ 3 \mid (k+1)^3 - (k+1)$

$3 \mid k^3 - k$
$3 \mid 3(k^2 + 1)$

$3 \mid k^3 - k + 3(k^2 + 1) \rightarrow 3 \mid k^3 + 3k^2 - k + 3 = (k+1)^3 - (k+1)$ ok