Fundamentals of Cryptography

Homework 3

Sepehr Ebadi **9933243**

Question 1

1)

در حالتی که صحت فرستنده پیام و حفظ یکپارچگی پیام (Authentication/Integrity) برایمان مهم باشد در مبحث رمز های قالبی باید از مود GCM استفاده بکنیم. دلیلش هم این است که این مود همانند مود های OFB و CFB و CTR برای ساخت یک استریم سایفر مورد استفاده قرار می گیرند که این باعث میشه از مزیت سرعت برای دیتای های با حجم بالا بتوان استفاده کرد. و همچنین به دلیل وجود تگ در این ساختار میتوان صحت فرستنده پیام را نیز تامین کرد و همچنین به دلیل داشتن IV و Counter می تواند برایمان یکپارچگی پیام را تامین کند. و چون میتوان قسمت های ساخت key stream را به صورت آفلاین محاسبه کنیم پس برای فایل های بزرگ بسیار کارآمد خواهد بود.

2)

چون در مود ECB بلوک ها از هم کاملا مستقل هستند اتکر میتواند یکی از بلوک های خود را مطابق با اهدافش جایگزین بلوک های اصلی کند و همچنین چون در این مود پیام ها تکراری خروجی های مشابه میدهد پس اتکر میتواند الگو را بدست بیاورد. (مثال بانک در کتاب)

به این منظور مود CBC چون بلوک ها را از طریق IV به هم به صورت زنجیر وار وصل میکند پس دیگر این نوع حمله امکان پذیر نخواهد بود.

IV در این مود نقش اساسی ایجاد میکند زیرا باعث میشود دیگر پیام های تکراری و مشابه خروجی های مشابه ندهد و اتکر دیگر نتواند الگو را بفهمد و چون باعث ایجاد زنجیره میشود اتکر دیگر نتواند حمله جانشینی را انجام دهد.

3)

triple encryption، به دلیل اینکه حالتی را فرض کنید که اتکر یک جفت پیام اصلی و پیام رمز شده را داشته باشد در این حالت ابتدا در فضای کلی کلید(L0) شروع به عملیات رمز نگاری میکند و این اطلاعات شامل کلید و متن رمز شده را در جدولی نگهداری میکند. سپس از طرف متن رمز شده شروع می کند و در فضای کلی کلید (R0) شروع به عملیات رمز گشایی می کند در این حالت هر بار چک میکند اگر با یکی از موجودیت های داخل جدول مطابقت داشت انگاه با احتمال خوبی کلید را پیدا کرده است.

به دلیل اینکه در این حالت اتکر باید ترکیبات مختلف سه تایی را بررسی کند حالات ممکن به طور چشم گیری افزایش می یابد پس در واقع تقریبا غیر ممکن می شود.

در این حالت طول کلید افزایش می یابد که این نیز دوباره باعث می شود فضای کلید بزرگتر شود.

و اتکر دیگر امکان ندارد این نوع حمله را بزند به دلیل سه تایی بودن ترکیبات نمی تواند به مقادیر میانی به صورت همزمان دسترسی داشته باشد.

Question 1

1)

در حالت ECB، هر بلوک از متن ساده به طور مستقل رمزنگاری می‌شود و الگویی بین بلوک‌های تکراری متن ساده در متن رمز شده قابل مشاهده است. اما از آنجا که کلید k بیت است، فضای جستجوی کلید شامل 2^k کلید ممکن می‌باشد.

برای اینکه یک رمز بلوکی را بتوانیم با جستجوی کامل بشکنیم، به حداقل یک جفت متن آشکار و متن رمز شده نیاز داریم که این جفت به ما امکان بررسی کلیدهای مختلف و مقایسه نتایج با متن رمز شده را می‌دهد.

بنابراین:

تعداد متن‌های آشکار و رمز شده مورد نیاز، یک جفت متن آشکار و متن رمز شده کافی است.

برای شکستن رمز بلوکی در بدترین حالت، باید تمام کلیدهای ممکن را امتحان کنیم، زیرا ممکن است کلید صحیح آخرین گزینه‌ای باشد که بررسی می‌شود. از این رو، تعداد گام‌های مورد نیاز در بدترین حالت برابر با تعداد کل کلیدهای ممکن است، یعنی 2^k

2)

در حالت CBC، هر بلوک از متن ساده قبل از رمزنگاری با استفاده از کلید، با بلوک قبلی از متن رمز شده (یا با IVبرای بلوک اول) ترکیب می‌شود. این ترکیب معمولاً با عملیات XOR انجام می‌شود. به دلیل این که بردار اولیه IVشناخته شده است، ساختار پیام را می توان برای جستجوی کلید از طریق جستجوی کامل کلید بررسی کرد.

برای انجام جستجوی تمام-کلیدی کافی است یک جفت متن آشکار و متن رمز شده داشته باشیم، زیرا از این طریق می‌توان با استفاده از IV عملیات را در بلوک اول بازسازی کرد و تمام کلیدهای ممکن را بررسی نمود.

بنابراین:

تعداد متون آشکار و متن‌های رمز شده مورد نیاز یک جفت متن آشکار و متن رمز شده کافی است.

در بدترین حالت، مشابه حالتECB ، نیاز است که تمام کلیدهای ممکن را بررسی کنیم. از این رو، تعداد گام‌های مورد نیاز در بدترین حالت برابر با تعداد کل کلیدهای ممکن، یعنی 2^k خواهد بود.

3)

در حالت CBC با جستجوی تمام‌کلیدی و در نبود IV، برای شناسایی کلید نیاز داریم که ترکیب کلید و IV به درستی شناسایی شود. از آنجا که IV در هر تلاش متفاوت می‌تواند باشد و ناشناخته است، نیاز داریم چندین جفت از متون آشکار و متون رمز شده را داشته باشیم تا بتوانیم تمامی ترکیب‌های ممکن از کلید و IV را آزمایش کنیم.

در عمل، برای جستجوی کلید در نبود IV

معمولاً ۲ تا ۳ جفت متن آشکار و متن رمز شده کافی است تا بتوانیم هم IV و هم کلید صحیح را شناسایی کنیم، زیرا هر جفت اضافی به محدود کردن فضای جستجو کمک می‌کند.

در بدترین حالت، ما همچنان باید تمامی کلیدهای ممکن را بررسی کنیم، که برابر با 2^k گام خواهد بود. اما به دلیل ناشناخته بودن IV، ممکن است نیاز باشد این تعداد گام‌ها برای هر IVممکن نیز تکرار شوند. اما از آنجا که چندین جفت متن آشکار و متن رمز شده داریم، در عمل این تعداد ترکیب به شدت محدود می‌شود.

Question 3

$m = 6 = 2\times3 \rightarrow \varphi(6) = (3-1) \times (2-1) = 2$

$a^2 \equiv 1 \bmod 6$, if $\gcd(a,6) = 1$

$\gcd(0,6) \neq 1$	$0^2 \equiv 0 \bmod 6$
$\gcd(1,6) = 1$	$1^2 \equiv 1 \bmod 6$
$\gcd(2,6) \neq 1$	$2^2 \equiv 4 \bmod 6$
$\gcd(3,6) \neq 1$	$3^2 \equiv 9 \equiv 3 \bmod 6$
$\gcd(4,6) \neq 1$	$4^2 \equiv 16 \equiv 4 \bmod 6$
$\gcd(5,6) = 1$	$5^2 \equiv 25 \equiv 1 \bmod 6$

$m = 9 \rightarrow \varphi(9) = 3_2 - 3_1 = 9-3 = 6$

$a^6 \equiv 1 \bmod 9$, if $\gcd(a,9) = 1$

$\gcd(0,9) \neq 1$	$0^6 \equiv 0 \bmod 9$
$\gcd(1,9) = 1$	$1^6 \equiv 1 \bmod 9$
$\gcd(2,9) = 1$	$2^6 \equiv 64 \equiv 1 \bmod 9$
$\gcd(3,9) \neq 1$	$3^6 \equiv (3_3)_2 \equiv 0_2 \equiv 0 \bmod 9$
$\gcd(4,9) = 1$	$4^6 \equiv (2_6)_2 \equiv 1_2 \equiv 1 \bmod 9$
$\gcd(5,9) = 1$	$5^6 \equiv 1 \bmod 9$
$\gcd(6,9) \neq 1$	$6^6 \equiv 2_6 \times 3_6 \equiv 1 \times 0 \equiv 0 \bmod 9$

$\gcd(7,9) = 1 \qquad 7^6 \equiv 1 \bmod 9$
$\gcd(8,9) = 1 \qquad 8^6 \equiv 1 \bmod 9$

Question 4

1)

$$\gcd(26,7) = sr_0 + tr_1$$
$$r_0 = 26, r_1 = 7$$
$$26 = 3 \times 7 + 5 \rightarrow 5 = 1r_0 - 3r_1$$
$$7 = 1 \times 5 + 2 \rightarrow 2 = r_1 - (r_0 - 3r_1) = -r_0 + 4r_1$$
$$5 = 2 \times 2 + 1 \rightarrow 1 = r_0 - 3r_1 - 2(-r_0 + 4r_1) = 3r_0 - 11r_1$$
$$s = 3, t = -11$$
$$t = a^{-1} = -11 \; mod \; 26 \equiv 15 \; mod \; 26$$

2)

$$\gcd(999,19) = sr_0 + tr_1$$
$$r_0 = 999, r_1 = 19$$
$$999 = 52 \times 19 + 11 \rightarrow 11 = 1r_0 - 52r_1$$
$$19 = 1 \times 11 + 8 \rightarrow 8 = -r_0 + 53r_1$$
$$11 = 1 \times 8 + 3 \rightarrow 3 = 2r_0 - 105r_1$$
$$8 = 2 \times 3 + 2 \rightarrow 2 = -5r_0 + 263r_1$$
$$3 = 1 \times 2 + 1 \rightarrow 1 = 7r_0 - 368r_1$$
$$s = 7, t = -368$$
$$t = a^{-1} = -368 \; mod \; 999 \equiv 631 \; mod \; 26$$

Question 5

1)

$$r_0 = 7469, r_1 = 2464$$
$$7469 \; mod \; 2464 = 77 \rightarrow \gcd(7469,2464) = \gcd(2464,77)$$
$$2464 \; mod \; 77 = 0 \rightarrow \gcd(2464,77) = \gcd(77,0) = 77$$

2)

$$r_0 = 4001, r_1 = 2689$$
$$4001 \; mod \; 2689 = 1312 \rightarrow \gcd(4001,2689) = \gcd(2689,1312)$$
$$2689 \; mod \; 1312 = 65 \rightarrow \gcd(2689,1312) = \gcd(1312,65)$$
$$1312 \; mod \; 65 = 12 \rightarrow \gcd(1312,65) = \gcd(65,12)$$

$65 \; mod \; 12 = 5 \; \rightarrow \gcd(65,12) = \gcd(12,5)$
$12 \; mod \; 5 = 2 \rightarrow \gcd(12,5) = \gcd(5,2)$
$5 \; mod \; 2 = 1 \rightarrow \gcd(5,2) = \gcd(2,1)$
$2 \; mod \; 1 = 0 \; \rightarrow \gcd(2,1) = \gcd(1,0) = 1$