حوری دهش 9821413

سوال 1:

Key: 9821413

Plaintext: “Let’s put a smile on that face”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key | 9 | 8 | 2 |  | 1 | 4 | 1 | 3 | 9 | 8 | 2 | 1 | 4 | 1 | 3 | 9 | 8 | 2 | 1 | 4 | 1 | 3 | 9 | 8 |
| Plaintext | l | e | t | ' | s | p | u | t | a | s | m | i | l | e | o | n | t | h | a | t | f | a | c | e |
| Ciphertext | u | m | v | ' | t | t | v | w | j | a | o | j | p | f | r | w | b | j | b | x | g | d | l | m |

Ciphertext: "Umv'ttvwjaojpfrwbjbxgdlm"

سوال 2:

در حمله Only Ciphertext چون ما Ciphertext را داریم پس باید Ciphertext را سه بار رمزگشایی کنیم یعنی از هر سه کلید باید استفاده کنیم تا به plaintext برسیم پس پیچیدگی حمله جستجوی فراگیر در این حالت میشود یعنی برای به دست اوردن سه کلید به زمان نیاز داریم

در حمله known plaintext چون ما plaintext را داریم، فقط از دو کلید استفاده میکنیم در نهایت پیچیدگی حمله جستجوی فراگیر برای پیدا کردن دو کلید میشود

سوال 3:

در حالت CBC بلوک‌های رمزگشایی شده یکی پس از دیگری به عنوان ورودی به بلوک‌های بعدی داده می‌شوند. این بدین معنی است که اگر یک کلید یا یک IV به طور مجدد استفاده شود، تأثیرات آن بر بلوک‌های بعدی انتقال داده شده به سادگی قابل مشاهده خواهد بود. به عبارت دیگر اگر برای بلوک‌های بعدی از همان کلید و IV قبلی استفاده شود به دلیل تکرار شدن IV و کلید، در برخی از حالات امنیت الگوریتم CBC کاهش پیدا می‌کند یعنی اگر بلوک‌های متنی مشابه در ورودی وجود داشته باشد، توابع XOR و رمزنگاری انجام شده برای هر دو بلوک، مشابه خواهد بود و ممکن است با تحلیل الگوی برخی از بلوک‌ها حملاتی با موفقیت نفوذ کنند.

سوال 4:

SIK: (3,5,12,23)

n=47

m=6

𝑀=1101

Public key:

3\*6 mod 47 = 18

5\*6 mod 47 = 30

12\*6 mod 47 = 25

23\*6 mod 47 = 44

(18,30,25,44)

Private key:

Ciphertext:

18+30+44 = 92

سوال 5:

حمله MITM به تبادل کلید Diffie-Hellman به رمزنگاری ECC زمانی رخ می دهد که یک مهاجم ارتباط بین دو طرف را رهگیری کرده و آن را تغییر دهد. در تبادل کلید ECC DH، آلیس و باب بر روی یک منحنی و یک نقطه پایه در منحنی توافق می کنند. هر کدام یک کلید خصوصی تولید کرده و از کلیدهای خصوصی خود و نقطه پایه برای تولید یک کلید عمومی استفاده می کنند. سپس طرفین کلید های عمومی خود را مبادله کرده و یک کلید مشترک را محاسبه می کنند که به عنوان کلید رمزگذاری متقارن استفاده می شود.

در حمله MITM به ECC DH، مهاجم ارتباط بین آلیس و باب را رهگیری می کند و هر یک از طرفین را به دیگری جعل می کند. مهاجم کلید عمومی خود را با استفاده از یک کلید خصوصی متفاوت تولید کرده و این کلید عمومی را طوری برای آلیس می فرستد که گویی کلید عمومی باب است. مهاجم همین کار را برای باب هم انجام می دهد و یک کلید عمومی متفاوت را به آلیس می فرستد که گویی کلید عمومی آلیس است.

وقتی آلیس و باب کلید مشترک خود را با استفاده از کلیدهای عمومی مهاجم محاسبه می‌کنند، مهاجم می‌تواند ارتباط بین آلیس و باب را رمزگشایی کرده بخواند و اصلاح کند که این کار را می تواند با کلید خصوصی خودش انجام دهد و سپس آن را با کلید عمومی خودش دوباره رمزگذاری کند و ان را به گیرنده مورد نظر منتقل کند.

سوال 6:

Alice sends Bob: 12(2,7) = (153,36)

Bob sends Alice: 31(2,7) = (103,153)

Alice sends Bob: 12(103,153) = (137,54)

Bob sends Alice: 31(153,36) = (137,54)

Key: (137,54)

سوال 7:

n = ((9821413 mod 5) + 2) = 5

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| z | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| z | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| z | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| z | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| z | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| z | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |

سوال 8:

ساختار گواهی X.509 شامل مجموعه ای از فیلدهای داده است که حاوی اطلاعاتی در مورد نهادی است که گواهی شناسایی می کند و همچنین اطلاعات مربوط به خود گواهی. مهم ترین فیلدهای داده در گواهی X.509 عبارتند از:

1- Version Number: این قسمت نشان دهنده نسخه استاندارد X.509 است که برای رمزگذاری گواهی استفاده شده است.

2- Serial Number: این فیلد حاوی یک شناسه منحصر به فرد است که توسط مرجع صدور گواهی (CA) اختصاص داده شده است تا گواهی را از سایر گواهی ها که صادر کرده است متمایز کند.

3- Signature Algorithm Identifier: این فیلد الگوریتم مورد استفاده توسط CA برای امضای گواهی را مشخص می کند، مانند RSA یا DSA.

4- Issuer Name: این فیلد حاوی نام CA است که گواهی را صادر کرده است.

5- Validity Period: این فیلد حاوی تاریخ هایی است که طی آن گواهینامه معتبر است از جمله تاریخ شروع و پایان.

6- Subject Name: این فیلد حاوی نام نهادی است که گواهینامه آن را شناسایی می کند مانند یک وب سایت یا یک فرد.

7- Subject Public Key Info: این فیلد حاوی اطلاعاتی درباره کلید عمومی مرتبط با موضوع است مانند الگوریتم مورد استفاده و خود کلید.

8- Certificate Extensions: این فیلد حاوی اطلاعات اضافی اختیاری درباره گواهی است مانند محدودیت‌های استفاده یا اطلاعات لغو گواهی.

9- Signature Value: این فیلد حاوی امضای دیجیتال گواهی است که با استفاده از کلید خصوصی CA ایجاد شده است.

هر یک از این فیلدهای داده با استفاده از یک نحو خاص که در استاندارد X.509 تعریف شده است کدگذاری می‌شوند و ساختار داده‌های حاصل به‌ صورت دیجیتالی توسط CA امضا می‌شود تا از صحت آن اطمینان حاصل شود. ساختار گواهی X.509 می تواند بسیار پیچیده باشد، اما برای فعال کردن ارتباط امن از طریق اینترنت ضروری است.

سوال 9:

سیستم رمز ECC یکی از روش‌های رمزنگاری کلید عمومی است که بر پایه منحنی‌های بیضوی (elliptic curves) ساخته شده است. در این سیستم برای ایجاد جفت کلید عمومی و خصوصی، ابتدا یک منحنی بیضوی تعریف می‌شود این منحنی بیضوی یک نقطه مبدا و یک نقطه پایانی دارد که با نام "نقطه بین‌دو" شناخته می‌شود.

در این روش از یک الگوریتم رمزنگاری کلید عمومی استفاده شده که با استفاده از منحنی بیضوی برای هر کاربر یک جفت کلید عمومی و خصوصی تولید می‌شود. برای تولید کلید عمومی یک نقطه اولیه در منحنی بیضوی انتخاب شده و بعد با تکراری از عملیات جمع نقطه‌ها، نقطه دیگری در منحنی بیضوی بدست می‌آید این نقطه جدید به عنوان کلید عمومی برای کاربر در نظر گرفته می‌شود.

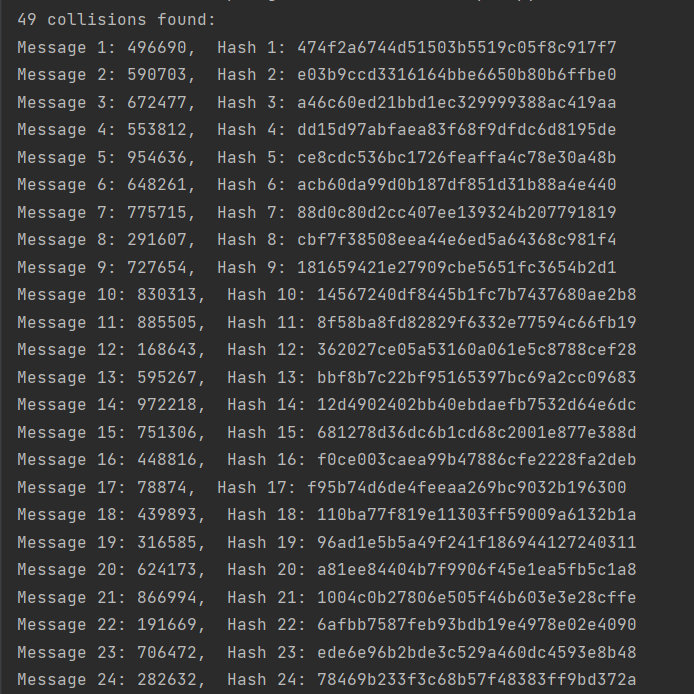
برای تولید کلید خصوصی کاربر باید برای خود یک عدد رندوم انتخاب کند با استفاده از این عدد و نقطه عمومی که قبلاً برای کلید عمومی تولید شده بود بازیابی نقطه‌ای از منحنی بیضوی صورت می‌گیرد که به عنوان کلید خصوصی برای کاربر در نظر گرفته می‌شود.

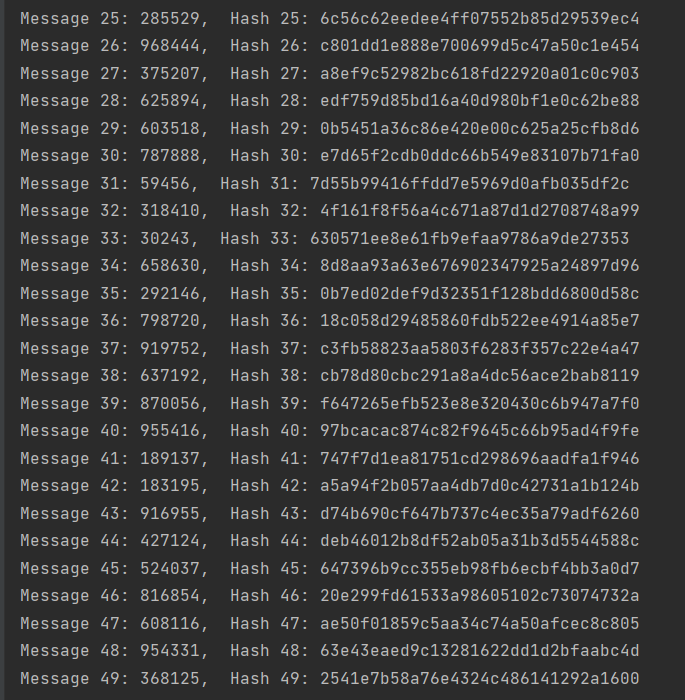
برای ارسال یک پیام رمزنگاری شده به دستگاه گیرنده، پیام با استفاده از کلید عمومی گیرنده رمزنگاری می‌شود. برای رمزگشایی پیام، دستگاه گیرنده از کلید خصوصی خود استفاده می‌کند تا پیام رمزگشایی شده را باز کند.

سوال 10:

توضیحات در خود کد داده شده است

خروجی کد:





سوال اضافه:

حمله lattice reduction به سیستم کوله پشتی یک تکنیک تحلیل رمزنگاری است که از نقاط ضعف در فرآیند رمزگذاری سیستم رمزنگاری کوله پشتی استفاده می کند. سیستم کوله پشتی از دنباله ای از اعداد صحیح به عنوان کلید عمومی استفاده می کند که از یک دنباله تصاعدی با استفاده از یک ضرب مخفی و محاسبات باقی مانده تولید می شود. فرایند رمزگذاری شامل تبدیل پیام متنی ساده به باینری و سپس ضرب هر بیت در بیت مربوطه در کلید عمومی و به دنبال ان جمع اوری محصولات است. حمله lattice reduction به سیستم کوله پشتی با ساختن یک lattice از کلید عمومی و سپس اعمال الگوریتم های lattice reduction برای حل مسئله جمع زیر مجموعه کار می کند. lattice با ایجاد یک ماتریس A که حاوی نمایش دودویی دنباله کلید عمومی است و سپس ساختن پایه ای برای lattice با استفاده از ستون های A ساخته می شود سپس الگوریتم‌های lattice reduction روی پایه اعمال می‌شوند تا پایه کوتاه‌ تر و متعامد تری پیدا کنند که بتوانند از ان برای حل مسئله جمع زیر مجموعه استفاده کرد. الگوریتم Lenstra-Lenstra-Lovaszیا LLL یکی از این الگوریتم هایی است که می توان برای این منظور استفاده کرد. هنگامی که lattice کاهش یافت، پایه ای پیدا می شود که کوتاه تر از پایه اصلی است. از این مبنا می توان برای حل مسئله جمع زیر مجموعه با یافتن یک نقطه lattice نزدیک به مجموع هدف استفاده کرد سپس نقطه lattice را می توان به یک راه حل برای مسئله جمع زیر مجموعه تبدیل کرد که می تواند برای بازیابی ضریب مخفی و رمزگشایی پیام استفاده شود.

برای محافظت در برابر حملات lattice reduction در سیستم کوله پشتی، می توان از اندازه های بزرگتر کلید استفاده کرد و کلید عمومی را می توان با استفاده از الگوریتم پیچیده تری که در برابر حملات lattice مقاوم است تولید کرد. یکی از این الگوریتم ها سیستم رمزنگاری کوله پشتی Chor-Rivest است که از یک جایگشت trapdoor برای تولید کلید عمومی استفاده می کند.