سوال ۱)

.۱

انتخاب حالت رمزنگاری: برای رمزنگاری فایل‌های بزرگ به گونه‌ای که هم محرمانگی و هم یکپارچگی حفظ شود، می‌توان از حالت GCM استفاده کرد. این حالت نه تنها داده‌ها را به صورت موازی رمزنگاری می‌کند که منجر به بهبود سرعت و عملکرد در سیستم‌هایی با حجم داده زیاد می‌شود، بلکه به دلیل ویژگی‌های ذاتی‌اش، یک کد احراز هویت پیام (MAC) نیز تولید می‌کند که تضمین‌کننده یکپارچگی پیام و احراز هویت فرستنده است. همچنین، حالت CBC با استفاده از یک بردار اولیه (IV) تصادفی نیز می‌تواند گزینه مناسبی باشد، زیرا این حالت با زنجیره کردن بلاک‌های متوالی از پیام، از تکرار بلاک‌های یکسان جلوگیری کرده و امنیت بیشتری نسبت به حالت ECB فراهم می‌کند.

.۲

مقاومت در برابر حملات: حالت ECB بسیار ضعیف است زیرا بلاک‌های یکسان از پیام اصلی را به بلاک‌های رمزنگاری شده یکسان تبدیل می‌کند. به عنوان مثال، اگر مهاجم به بخشی از پیام اصلی دسترسی داشته باشد، می‌تواند با مقایسه الگوهای بلاک‌های رمزنگاری شده، به اطلاعات بیشتری دست یابد و حمله جایگزینی را انجام دهد. در مقابل، حالت CBC با استفاده از یک بردار اولیه (IV) و زنجیره کردن بلاک‌ها از این مشکل جلوگیری می‌کند. در حالت CBC، هر بلاک با استفاده از بلاک قبلی رمزنگاری می‌شود و IV به عنوان یک مقدار تصادفی در ابتدای پیام اضافه می‌شود، که این باعث می‌شود حتی اگر دو بلاک از پیام اصلی یکسان باشند، بلاک‌های رمزنگاری شده متفاوت تولید شود.

.۳

رمزنگاری چندگانه و اثربخشی آن: استفاده از Triple Encryption بسیار امن‌تر از رمزنگاری دوگانه است. در رمزنگاری دوگانه، حمله Meet-in-the-Middle می‌تواند امنیت سیستم را تهدید کند. این حمله با استفاده از جستجوی دو مرحله‌ای، فضای کلیدی را به شدت کاهش می‌دهد. در مقابل، رمزنگاری سه‌گانه با استفاده از سه کلید مختلف (یا دو کلید متفاوت)، باعث می‌شود که چنین حملاتی موفق نباشند و امنیت به طور قابل توجهی افزایش یابد.

سوال ۲)

.۱

با توجه به این‌که طول کلید از طول بلوک (بر حسب بیت) کمتر است، ممکن است که بر اساس اصل لانه کبوتری، هر کلید به یک متن رمز شده یکتا نگاشت شود؛ ولی این امکان هم وجود دارد که چند کلید به یک متن رمز شده نگاشت شوند. اگر t را تعداد جفت‌های plaintext و ciphertext مورد استفاده برای شکستن رمز در نظر بگیریم، احتمال پیدا کردن یک کلید مثبت کاذب برابر است با : 2^{k-tn} . بنابراین بسته به مقادیر n و k ، اگر از دو جفت plaintext و ciphertext استفاده کنیم، احتمال بدست آوردن کلید کاذب بسیار کم شده و اطمینان بیشتری بدست می‌آید. در صورتی که آخرین کلید مورد بررسی درست باشد، بدترین حالت، باید 2^k کلید را چک کنیم.

.۲

با دانستن بردار اولیه (IV) در مد CBC، شکستن رمز همانند مد ECB شده و تفاوت چندانی ندارد. تنها تفاوت بین این دو مد، وجود XOR در مد CBC است که باید قبل از هر بررسی با i-1 اُمین متن رمزشده یا IV انجام شود؛ که این یک افزایش ناچیز در هزینه می‌باشد. بنابراین بسته به مقادیر n و k ، اگر از دو جفت plaintext و ciphertext استفاده کنیم، احتمال بدست آوردن کلید کاذب کمتر شده و اطمینان بیشتری بدست می‌آید. همچنین در بدترین حالت نیاز است که 2^k کلید را چک کنیم.

.۳

ندانستن بردار اولیه (IV) به این معنی است که نمی‌دانیم چه برداری قبل از رمزگذاری با متن اصلی XOR شده است. اگر دو جفت plaintext و ciphertext داشته باشیم؛ می‌توانیم از ciphertext بلوک اول به عنوان IV برای بلوک دوم استفاده کنیم و سپس مشابه با قسمت های قبلی، با جستجو کلید را بدست آورده و در نهایت اولین بلوک را توسط کلید رمزگشایی کرده و مقدار IV را بدست آوریم. با داشتن جفت سوم plaintext و ciphertext، می‌توان نتایج را بررسی و سطح اطمینان بالاتری بدست آورده و همچنین احتمال بدست آوردن کلید کاذب را بسیار کمتر کنیم.

.۴

در حالتی که مقدار IV شناخته شده است، تنها تفاوت در هزینه محاسبه XOR برای هر بلوک در مد CBC است. در حالتی که مقدار IV ناشناخته است، برای رسیدن به یک سطح اطمینان برابر، در مد CBC نیاز به یک جفت plaintext و ciphertext بیشتر نسبت به مد ECB داریم. (به عبارتی دیگر با داشتن تعداد t جفت plaintext و ciphertext در هر دو مد، سطح اطمینان مد ECB برابر با t و سطح اطمینان مد CBC برابر با t-1 می‌باشد)

سوال ۳)

.۱

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

قضیه اویلر:

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

$\gcd(0,6) \neq 1 \qquad 0^2 \equiv 0 \bmod 6$

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

$\gcd(2,6)\neq 1 \qquad 2^2 \equiv 4 \bmod 6$

$\gcd(3,6) \neq 1 \qquad 3^2 \equiv 9 \equiv 3 \bmod 6$

$\gcd(4,6) \neq 1 \qquad 4^2 \equiv 16 \equiv 4 \bmod 6$

$\gcd(5,6)=1 \qquad 5^2 \equiv 25 \equiv 1 \bmod 6$

۲.

$m = 9 \rightarrow \quad \varphi(9) = 3^2 - 3^1 = 9 - 3 = 6$

قضیه اویلر:

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

$\gcd(0,9) \neq 1 \qquad 0^6 \equiv 0 \bmod 9$

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

$\gcd(2,9) = 1 \qquad 2^6 \equiv 64 \equiv 1 \bmod 9$

$\gcd(3,9) \neq 1 \qquad 3^6 \equiv (3^3)^2 \equiv 0^2 \equiv 0 \bmod 9$

$\gcd(4,9) = 1 \qquad 4^6 \equiv (2^6)^2 \equiv 1^2 \equiv 1 \bmod 9$

$\gcd(5,9) = 1 \qquad 5^6 \equiv 1 \bmod 9$

$\gcd(6,9) \neq 1 \qquad 6^6 \equiv 2^6 \times 3^6 \equiv 1 \times 0 \equiv 0 \bmod 9$

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

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

سوال ۴)

۱.

$\gcd(26,7) = 1$ ← معکوس ضربی وجود دارد.

$r_0 = 26 , r_1 = 7 \qquad (26,7)$

$26 = 3\times7+5 \quad (7,5) \qquad 5 = 26 - 3\times7 = r_0 - 3r_1$

$7 = 1\times5+2 \quad (5,2) \qquad 2 = 7 - 1\times5 = r_1 - 1(r_0 - 3r_1) = 4r_1 - r_0$

$5 = 2\times2+1 \quad (2,1) \qquad 1 = 5 - 2\times2 = (r_0 - 3r_1) - 2(4r_1 - r_0) = -11r1 + 3r0$

$\rightarrow 1 = -11\times7 + 3\times26$

$\rightarrow 7^{-1} \equiv -11 \bmod 26 = \mathbf{15}$

i	**q_{i-1}**	**r_i**	**s_i**	**t_i**
2	3	5	1	-3
3	1	2	-1	4
4	2	1	3	**-11**

.۲

$gcd(999,19) = 1$ ← معکوس ضربی وجود دارد.

$r_0 = 999$, $r_1 = 19$ (999,19)

$999 = 52\times19+11$ (19,11) $11 = 999 - 52\times19 = r_0 - 52r_1$

$19 = 1\times11+8$ (11,8) $8 = 19 - 1\times11 = r_1 - (r_0 - 52r_1) = 53r_1 - r_0$

$11 = 1\times8+3$ (8,3) $3 = 11 - 1\times8 = (r_0 - 52r_1) - (53r_1 - r_0) = 2r_0 - 105r_1$

$8 = 2\times3+2$ (3,2) $2 = 8 - 2\times3 = (53r_1 - r_0) - 2(2r_0 - 105r_1) = 263r_1 - 5r_0$

$3 = 1\times2+1$ (2,1) $1 = 3 - 1\times2 = (2r_0 - 105r_1) - (263r_1 - 5r_0) = -368r_1 + 7r_0$

$\rightarrow 1 = -368\times19 + 7\times999$

$\rightarrow 19^{-1} \equiv -368 \bmod 999 = \mathbf{631}$

i	**q_{i-1}**	**r_i**	**s_i**	**t_i**
2	52	11	1	-52
3	1	8	-1	53
4	1	3	2	-105
5	2	2	-5	263
6	1	1	7	**-368**

سوال ۵)

.۱

$r_0 = 7469$, $r_1 = 2464$

$7469 = 3 \times 2464 + 77$	$gcd(7469, 2464) = gcd(2464, 77)$
$2464 = 32 \times 77 + 0$	$gcd(2464, 77) = gcd(77, 0) = 77$

.۲

$r_0 = 4001$, $r_1 = 2689$

$4001 = 1 \times 2689 + 1312$	$gcd(4001, 2689) = gcd(2689, 1312)$
$2689 = 2 \times 1312 + 65$	$gcd(2689, 1312) = gcd(1312, 65)$
$1312 = 20 \times 65 + 12$	$gcd(1312, 65) = gcd(65, 12)$
$65 = 5 \times 12 + 5$	$gcd(65, 12) = gcd(12, 5)$
$12 = 2 \times 5 + 2$	$gcd(12, 5) = gcd(5, 2)$
$5 = 2 \times 2 + 1$	$gcd(5, 2) = gcd(2, 1)$
$2 = 2 \times 1 + 0$	$gcd(2, 1) = gcd(1, 0) = 1$