جواب سوال ۱

جواب سوال ۲

بخش اول

وقتی یک پیام m ابتدا توسط الگوریتم فشرده‌سازی C(m) فشرده می‌شود و سپس با استفاده از رمزنگاری بلوکی با اندازه بلوک ۸ بیت پد شده و رمزگذاری می‌گردد، طول نهایی پیام رمزگذاری شده مستقیماً به طول پیام فشرده شده C(m) بستگی دارد. مهاجم که تنها تعداد بلوک‌های ارسال شده را مشاهده می‌کند، می‌تواند اطلاعاتی درباره طول C(m) به دست آورد. از آنجایی که طول C(m) نشان‌دهنده تعداد و طول رشته‌های ۱ متوالی در پیام اصلی m است، مهاجم می‌تواند استنتاج‌هایی درباره الگوی تکراری در m انجام دهد.

با یک مثال درباره‌ی این مورد بیشتر توضیح می‌دهم. **مثال:**

پیام $m_۱$: ۱۱۱۱۱۱۱۱۱۱۱۰۱۱۱۱۱۰۱۰۱۱۱

$C(m_۱) =$ ۱۰۱۰۰۱۰۱۰۰۰۱۰۰۱۱

طول $C(m_۱) =$ ۱۶ بیت $\rightarrow$ ۲ بلوک ۸ بیتی

پیام $m_۲$: ۱۱۱۱۱۰۱۱۱۱۱۱۰۱۱۱۱۱۰۱۱۱۱

$C(m_۲)$ ممکن است طول بیشتری داشته باشد (فرضاً ۲۴ بیت) $\rightarrow$ ۳ بلوک ۸ بیتی

در این حالت، اگر مهاجم مشاهده کند که دو بلوک ارسال شده‌اند، احتمال می‌دهد پیام $m_۱$ با الگوی تکراری مناسب فشرده شده است. اگر سه بلوک ارسال شود، ممکن است پیام $m_۲$ با الگوی کمتر تکراری فشرده شده باشد.

بخش دوم

مهاجم می‌تواند از تفاوت‌های فشرده‌سازی بین دو پیام با طول اصلی برابر استفاده کند تا تشخیص دهد کدام پیام رمزگذاری شده است. اگر دو پیام $m_۱$ و $m_۲$ دارای طول اصلی یکسان باشند اما الگوهای متفاوتی از رشته‌های ۱ متوالی داشته باشند، فشرده‌سازی آن‌ها نیز متفاوت خواهد بود. پیام با الگوی فشرده‌تر (بیشتر رشته‌های تکراری و طولانی‌تر ۱ ها) منجر به $C(m)$ کوتاه‌تر و در نتیجه تعداد بلوک‌های کمتر خواهد شد.

با یک مثال درباره‌ی این مورد بیشتر توضیح می‌دهم. **مثال:**

پیام $m_۱$: ۱۱۱۱۱۱۱۱۱۱۱۰۱۱۱۱۱۰۱۰۱۱۱

$C(m_۱) =$ ۱۰۱۰۰۱۰۱۰۰۰۱۰۰۱۱

تعداد بلوک‌های رمزگذاری شده: ۲ بلوک

پیام $m_۲$: ۱۱۱۱۱۰۱۱۱۱۱۰۱۱۱۱۱۰۱۱۱۱

$C(m_۲) =$ ۱۰۱۰۱۰۱۰۰۱۰۱۰۱۰۱

تعداد بلوک‌های رمزگذاری شده: ۳ بلوک

در این حالت، اگر مهاجم مشاهده کند که تعداد بلوک‌های رمزگذاری شده ۲ بلوک است، نتیجه می‌گیرد که پیام $m_۱$ رمزگذاری شده است. اگر ۳ بلوک مشاهده کند، نتیجه می‌گیرد که پیام $m_۲$ رمزگذاری شده است.

این روش به مهاجم اجازه می‌دهد تا با تحلیل طول پیام‌های رمزگذاری شده و مقایسه آن‌ها با الگوهای مختلف فشرده‌سازی، اطلاعاتی درباره محتوای پیام اصلی بدست آورد. این نوع حمله نشان‌دهنده آسیب‌پذیری‌های احتمالی در ترکیب فشرده‌سازی و رمزنگاری است که پس از حملات CRIME در پروتکل‌های جدید مانند TLS 1.3 حذف شده‌اند تا از چنین تهدیداتی جلوگیری شود.

جواب سوال ۳

جواب سوال ۴