# مبانی امنیت – تمرین شماره ۲

**دکتر شهریاری**

## سوال اول

افزایش تعداد کاراکتر ها از ۲۶ به ۵۲ تغییر خیلی جزئی بوده و تاثیر خاصی ندارد. در حقیقت استفاده از کاراکتر های بزرگ انگلیسی می تواند فضای جست و جو برای یافتن mapping ها را کاهش نیز دهد، زیرا کاراکتر های بزرگ همیشه در ابتدا کلمات استفاده می شود و باعث می شود این کاراکتر ها سریع تو فاش شوند. بقیه تحلیل الگو ها مانند روش قبلی با ۲۶ کاراکتر کوچک است.

نتیجه گیری: اگرچه استفاده از ۵۲ کاراکتر بجای ۲۶ کاراکتر نیاز به computation بیشتری از سمت سخت افزار دارد، اما با توجه به سخت افزار های پیشرفته کنونی این نیازمندی تفاوت خاصی ایجاد نمیکند و از طرفی یافتن الگو های کاراکتر های بزرگ ساده تر هم می شود (بالاتر توضیح داده شد)

## سوال دوم

**الف)** برای ارتباط داشتن این ۱۰۰ نفر با یکدیگر، مانند گراف کامل با ۱۰۰ vertex عمل میکنیم که ۹۹ edge خواهد داشت. پس به $\frac{100\times99}{2}$ یعنی ۴۹۵۰ کلید متقارن نیاز خواهیم داشت، زیرا هر دو نفر به یک کلید نیاز دارند.

**ب)** ۱۰۰ کلید. زیرا مدیر به هر نفر یک کلید دارد و ۱۰۰ نفر داریم، پس کلا ۱۰۰ کلید نیاز داریم.

## سوال سوم

حملات cryptanalytic به پنج دسته تقسیم می شوند:

- Known-Plaintext Analysis (KPA): در این روش، مهاجم تعدادی متن رمزنگاری شده (ciphertext) و نشده (crib) دارد که به یکدیگر map شده اند و با تحلیل این متن ها و یافتن الگو های تکرار شونده مهاجم می تواند الگوریتم با بشکند. این روش ساده ترین روش است.
- Chosen-Plaintext Analysis (CPA): در این روش مهاجم می تواند تعدادی متن شانسی (crib) را به سیستم داده و متن رمزنگاری شده (ciphertext) را دریافت کند.
- Man-In-The-Middle (MITM) attack: در این روش مهاجم بین دو سیستم ارتباطی قرار گرفته و پیام ها/کلید ها را شنود می کند.
- Ciphertext-Only Analysis (COA): در این روش مهاجم متن اصلی (crib) را نداشته اما تعدادی متن رمزنگاری شده (ciphertext) دارد که با کمک آنها سعی بر یافتن متن های اصلی و الگوریتم رمزنگاری دارد. این سخت ترین و متداول ترین روش است.
- Adaptive Chosen-Plaintext Analysis (ACPA): این روش مشابه CPA است اما در اینجا مهاجم به صورت real-time می تواند متن های دلخواه خود را با توجه به خروجی سیستم انتخاب و دوباره به سیستم بدهد. اینجا مهاجم میتواند با آزمون و خطا کردن های هوشمندانه تر نسبت به CPA حملات خود را انجام دهد.

## سوال چهارم

در ابتدا نیاز به یک جدول برای encrypt کردن نیاز داریم:

# مبانی امنیت – تمرین شماره ۲

**دکتر شهریاری**

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

سپس متن را نوشته و کلید را به اندازه طول کلمه تکرار می کنیم:

| Input | l | i | f | e | | i | s | | f | u | l | l | | o | f | | s | u | r | p | r | i | s | e | s |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key | H | E | A | L | | T | H | | H | E | A | L | | T | H | | H | E | A | L | T | H | H | E | L |
| Output | S | M | F | P | | B | Z | | J | U | W | E | | V | J | | S | F | K | W | V | I | D | X | Z |

و سپس مطابق جدول جایگزین میکنیم. برای مثال خروجی ستون اول برابر s شده و خروجی ستون دوم برابر m می شود. این روند را برای تمامی حروف تکرار کرده و خروجی مطلوب:

smfp bz juwe vj sfkwvidxz

## سوال پنجم

دلیل استفاده چندین جدول برای DES آن است که امنیت آن افزایش پیدا کند. طبق کتاب Applied Cryptography اگر تعداد لایه ها کمتر از ۱۶ باشد به راحتی قابل شکست توسط Brute Force است، پس نه تنها باید تعداد را افزایش داد بلکه بهتر است از چندین جدول استفاده شود. اما برای AES به دلیل داشتن عملیات های بیشتر در همان یک جدول، نیازی به جداول بیشتر نیست و به تنهایی قابل اتکا است، اما همچنان می تواند به تعداد جداول آن اضافه کرد.

این رابطه امنیت بیشتر AES را نسبت به DES را نشان میدهد، زیرا رمزنگاری صرفا به تعداد لایه ها نیست، بلکه به پیچیدگی الگوریتم است. افزایش تعداد لایه ها سرعت را کاهش می دهد، درصورتی که میتوان امنیت و سرعت را با پیچیدگی الگوریتم جبران کرد.

## سوال ششم

زیرا روش CFB از نوع streaming است، یعنی به صورت real-time رمزنگاری انجام می شود که باعث شده هر بلوک به بلوک های پیشین وابسته باشد. این وابستگی امکان خطای propagation را بوجود می آورد. دلیل ریاضی این موضوع $Ci=Ek(Ci-1 \oplus Pi)$ است زمانی که Pi برابر بلوک متن صریح و Ci برابر بلوک متن رمزنگاری شده است.

پس هر بلوک، روی بلوک های بعدی تاثیر گذاشته و این تاثیر انتقال میابد. به همین خاطر است که vector اولیه باید با دقت انتخاب شود تا غیرقابل پیشبینی باشد و الگو تکرار شونده ای درون آن نداشته باشیم، زیرا این الگو به بلوک های بعد هم سرایت می کند.

# مبانی امنیت – تمرین شماره ۲

**دکتر شهریاری**

## سوال هفتم

ورودی 1100100111010101 است.

۱.در قدم اول ورودی را دو بخش میکنیم:

$$L0 = \ 11001001$$

$$R0 = \ 11010101$$

۲. در قدم بعدی R0 را داخل F() برده و خروجی را داخل E ذخیره میکنیم:

$$F(R0, K) = F(11010101, 1101) = \ 00000101 = E$$

۳. مقادیر L1 و R1 را محاسبه و ذخیره میکنیم:

$$L1 = R0 = \ 11010101$$

$$R1 = L0 \ XOR \ E = \ 11001001 \text{ XOR } 00000101 = \ 11001100$$

۴. خروجی:

$$L1 \ CONCAT \ R1 = \ 1101010111001100$$

## سوال هشتم

با چشم پوشی از کلید (برای الان) میخواهیم اثبات کنیم:

$$EP(A') = EP'(A)$$

برای اثبات این سوال در ابتدا داریم:

$$A' = A \ XOR \ 1$$

و همچنین برای XOR کردن دو متغیر:

$$A \ XOR \ B = \ 1 \ XOR \ A \ XOR \ 1 \ XOR \ B = A' \ XOR \ B'$$

پس اگر C خروجی *EP(A,K)* باشد، لزوما خروجی *EP(A',K')* نیز معادل C می شود و در مرحله جای گشت هیچ کدام از ورودی و کلید مکمل نمیشوند.