دانشکده مهندسی کامپیوتر

استاد درس: دکتر دیانت

بهار ۱۴۰۲

امنیت شبکه

یاسمین مدنی - پریسا ظفری

۱ حملات به DES

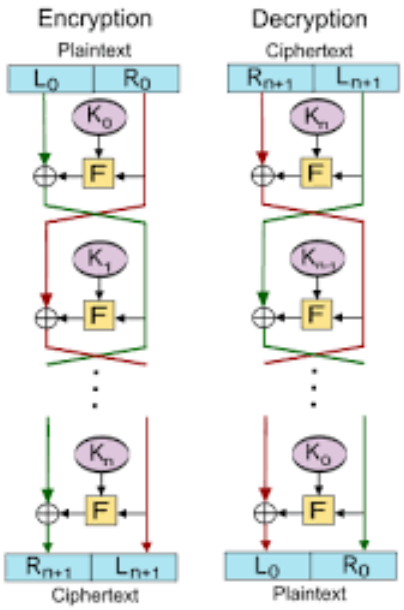
در طی سال های مختلف حملات مختلفی به DES صورت گرفته است . معروف ترین حملات با brute-force ،Differential cryptanalysis ،Linear cryptanalysis و Davies Attack صورت گرفته است.

۲ Differential cryptanalysis

تحلیل رمزی تفاضلی روشی است که تأثیر تفاوت‌های خاص در جفت‌های متن ساده بر تفاوت‌های جفت‌های متن رمزی حاصل را تحلیل می‌کند. از این تفاوت ها می توان برای تخصیص احتمالات به کلیدهای ممکن و یافتن محتمل ترین کلید استفاده کرد. رمزگشایی تفاضلی معمولاً روی بسیاری از جفت‌های متن ساده با همان تفاوت خاص فقط با استفاده از جفت‌های متن رمزی حاصل کار می‌کند. برای سیستم‌های رمزنگاری مشابه DES، این تفاوت به عنوان یک مقدار XOR ثابت دو متن ساده انتخاب می‌شود.

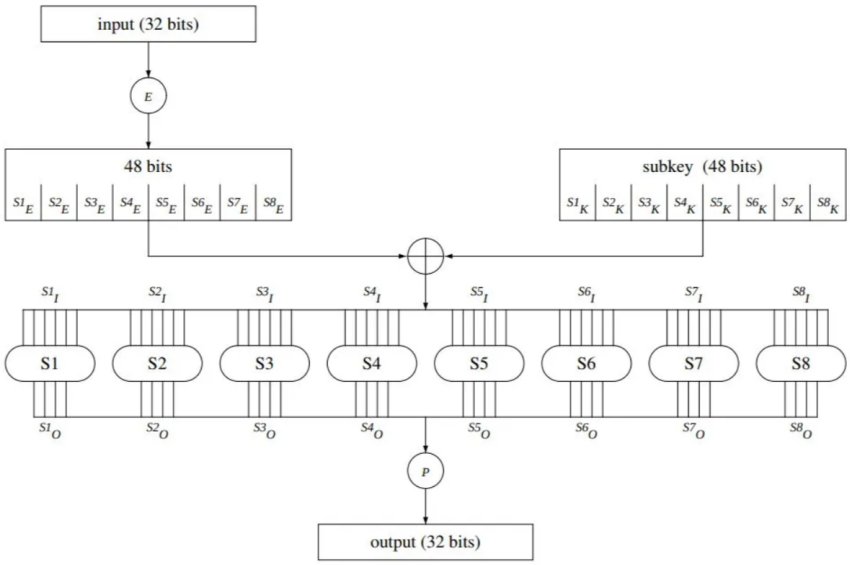
۱.۲ ساختار Feistel

این یک مدل طراحی است که رمزهای بلوکی مختلفی از آن مشتق شده است. DES یکی از این رمزهای بلوکی است. مدل Feistel برای DES ۶۴ بیت متن ساده را می گیرد و آن را به دو نیم تقسیم می کند، L و R هر کدام ۳۲ بیت. R۲ به صورت $L \oplus (R, Key)$ محاسبه می شود و L۲ همان R است. در اینجا، Key یک کلید ۴۸ بیتی است که از الگوریتم زمان بندی کلید مشتق شده است. این مدل در شکل زیر نشان داده شده است.



شکل ۱: Feistel

در یک الگوریتم رمزگذاری، این روش تبدیل متن ساده را می توان برای هر تعداد بار استفاده کرد. خروجی یک دور به عنوان ورودی دور بعدی در نظر گرفته می شود. این کار برای ۱۶ دور در DES استاندارد انجام می شود. f دارای ساختار زیر در DES است.



شکل ۲: Function F

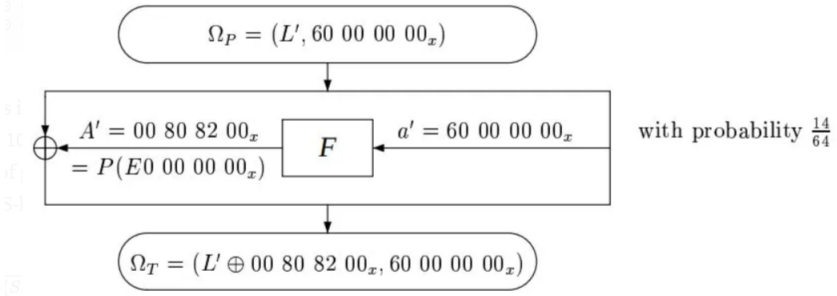
۲.۲ نمادها

- n_X یک عدد هگزادسیمال با زیرنویس x نشان داده می شود $10_x = 16$
- X ، X' در هر مرحله میانی در طول رمزگذاری جفت پیام، X۱ و X۲ مقادیر میانی متناظر دو اجرای الگوریتم هستند. X'=X1 $\oplus X2$
- P متن ساده با P نشان داده می شود.
- T متن رمز شده با T نشان داده می شود.
- P(X): جایگشت P با P(X) نشان داده می شود. توجه داشته باشید که P به عنوان یک متغیر متن ساده را نشان می دهد.
- E(X): بسط E با E(X) نشان داده می شود.
- IP(X): جایگشت اولیه.
- (L, R): نیمه چپ و راست متن ساده P (پس از جایگشت اولیه) به ترتیب با L و R نشان داده می شوند.
- (l, r): نیمه چپ و راست متن رمزی T (قبل از جایگشت نهایی) به ترتیب با l و r نشان داده می شوند.

- a,...., j: ورودی های ۳۲ بیتی تابع f در دورهای مختلف.
- A,...., J: خروجی های ۳۲ بیتی تابع f در دورهای مختلف

۳.۲ مشخصه

با هر جفت رمزگذاری، مقدار XOR دو متن ساده آن، XOR متن رمزی آن، XOR ورودی هر دور در دو اجرا، و XOR خروجی هر دور در دو اجرا مرتبط است. این مقادیر XOR یک مشخصه n دور را تشکیل می دهند. یک مشخصه یک احتمال دارد، که احتمال این است که یک جفت تصادفی با متن ساده XOR انتخاب شده دارای هایXOR گرد و متن رمزی مشخص شده در مشخصه باشد. ما متن های ساده XOR یک مشخصه را با Ω_p و متن های رمزی آن را با Ω_t نشان می دهیم. توجه داشته باشید که این احتمال به دلیل وجود جفت ورودی های مختلف با XOR یکسان ممکن است به خروجی XOR متفاوت منجر شود.
برای توضیح ، یک مثال آورده شده است.



شکل ۳: example

$$a^{'}=0110\ \ 0000\ \ 0000\ \ 0000\ \ 0000\ \ 0000\ \ 0000\ \ 0000$$
$$E(a^{'})=001100\ \ 000000\ \ 000000\ \ 000000\ \ 000000\ \ 000000\ \ 000000\ \ 000000$$

برای S۲-S۸ به عنوان ورودی XOR ۰ است، بنابراین خروجی XOR ۰ خواهد بود. اما، برای S۱، از آنجایی که ورودی XOR ۰۰۱۱۰۰ است، توزیع زیر خروجی XOR ایجاد می شود. بنابراین، احتمال به دست آوردن "E" ۷/۳۲ (یعنی ۱۴/۶۴) است. جایگشت P، هنگامی که به خروجی S-box اعمال می شود، $A^{'}$ $= (00808200)_x$ را نشان می دهد.

Output XOR ($S1'_O$)	Possible Input Pairs ($S1_I$)
3	(10,1C), (14,18), (24,28). (31,3D)
5	(00,0C), (15,19), (16,1A)
6	(07,0B), (20,2C), (33,3F)
9	(05,09), (11,1D), (35,39)
10	(22,2E), (30,3C), (34,38)
11	(23,2F), (27,2B)
12	(02,0E), (25,29), (32,3E)
13	(01,0D), (12,1E), (36,3A)
E	(03,0F), (06,0A), (13,1F), (17,1B), (21,2D), (26,2A), (37,3B)
F	(04,08)

شکل ۴: Possible input values for S1' XOR output by ۰۰۱۱۰۰ = (in hexadecimal)

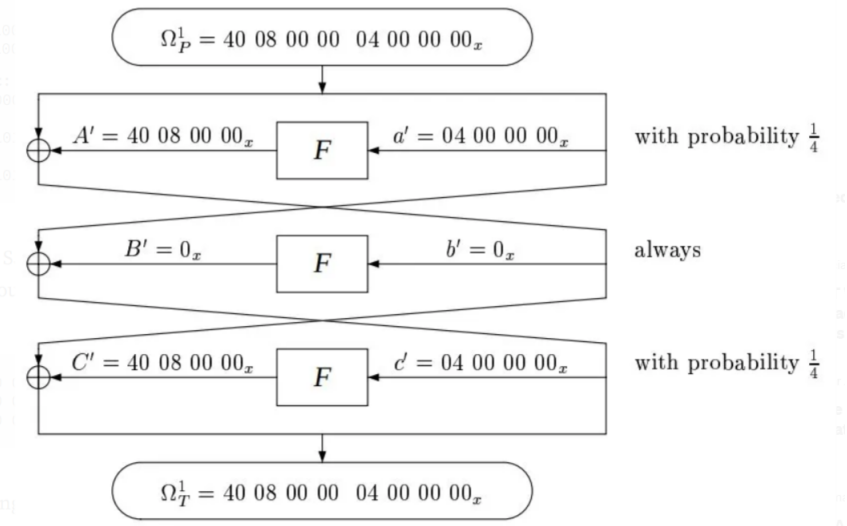
۳ Breaking DES reduced to 6 rounds

پس از تعریف مفهوم جفت ها و ویژگی ها، توضیح می دهیم که چگونه می توان از آن برای شکستن DES به ۶ دور استفاده کرد. ما از دو مشخصه ۳ دور استفاده می کنیم، هر دو با احتمال ۱/۱۶ و کلید را انتخاب می کنیم که اغلب شمارش می شود. هر یک از مشخصه ها به ما کمک می کند تا ۳۰ بیت کلید دور ۶ را پیدا کنیم. با این حال، ۳ تا از جعبه های S رایج هستند، بنابراین ما فقط ۴۲ بیت داریم. بقیه ۱۴ بیت را می توان با جستجوی جامع پیدا کرد.

فرض کنید که متن رمزی متن ساده داده شده را می دانیم (به یاد داشته باشید که در حال تلاش برای حمله متن ساده انتخابی هستیم). می دانیم که DES ۶ دور است و همچنین کلید:

Key : 111011110011001101110110110111100011010001010111111100010001001 1

مشخصه اول به صورت زیر است.



شکل ۵: مشخصه اول

ما متن‌های ساده را طوری انتخاب می‌کنیم که ورودی XOR بعد از جایگشت اولیه (IP) به صورت $(4008000004000000)_x$ باشد. توجه داشته باشید که $P1 \oplus P2$ با مشخصه یکسان نیست، اما $IP(P1) \oplus IP(P2)$ برابر با مشخصه است.

$P_1 = 1101010100100010110100110111001011100001101111000011001000101010$
$P_2 = 1101010100100010010100110110001011100001101111000111001000101010$

مشخصه:

0100000000001000000000000000000000001000000000000000000000000000

P_1 پس از جایگشت IP:

0001110101101101001000010001010100110101111110101010000011001110

P_2 پس از جایگشت IP:

0101110101100101001000010001010100110001111110101010000011001110

پنج S-box $(S2, S5, S6, S7, S8)$ در دور چهارم دارای XOR ورودی صفر هستند و بنابراین XOR خروجی آنها صفر است.

$$d^{'} = (40080000)_x$$
$$d^{'} = 0100 \quad 0000 \quad 0000 \quad 1000 \quad 0000 \quad 0000 \quad 0000 \quad 0000$$
$$E(d^{'}) = 001000 \quad 000000 \quad 000001 \quad 010000 \quad 000000 \quad 000000 \quad 000000 \quad 000000$$

های XOR خروجی مربوطه در دور ششم را می توان با $F^{'} = c^{'} \oplus l^{'}$ پیدا کرد.

$$l^{'} = F^{'} \oplus e^{'}$$
$$e^{'} = D^{'} \oplus c^{'}$$
$$F^{'} = D^{'} \oplus c^{'} \oplus l^{'}$$
از این رو، $F^{'} = c^{'} \oplus l^{'}$ برای s-box ۵

با دانستن متن رمز شده برای P_1 و P_2 به صورت زیر:
$T_1 = 01010100110001100110010111010111100100011101011101110110010011 10$
$T_2 = 11100100001101000011111110000010010101100111001101010000110100 10$
برای خنثی سازی اثر جایگشت نهایی اعمال شده در دور آخر، IP را اعمال می کنیم.
$T_1 = 11101111011110011110111100111100001110100100010010000000111010 10$
$T_2 = 11110001111101100001011100100100100010010010011100000010010111 100$
حالا ۳۲ بیت اول را به صورت f و ۳۲ بیت آخر را به صورت l استخراج میکنیم.

$$f_1 = 0011 \quad 1010 \quad 0100 \quad 0100 \quad 1000 \quad 0000 \quad 1110 \quad 1010$$
$$f_2 = 1000 \quad 1001 \quad 0010 \quad 0111 \quad 0000 \quad 0100 \quad 1011 \quad 1100$$
$$l_1 = 0011 \quad 1010 \quad 0100 \quad 0100 \quad 1000 \quad 0000 \quad 1110 \quad 1010$$
$$l_2 = 1000 \quad 1001 \quad 0010 \quad 0111 \quad 0000 \quad 0100 \quad 1011 \quad 1100$$

ورودی های s-box

$$E(f_1) =$$
$$000111 \quad 110100 \quad 001000 \quad 001001 \quad 010000 \quad 000001 \quad 011101 \quad 010100$$
$$E(f_2) =$$
$$010001 \quad 010010 \quad 100100 \quad 001110 \quad 100000 \quad 001001 \quad 010111 \quad 111001$$
$$c^{'} = 0000 \quad 0100 \quad 0000 \quad 0000 \quad 0000 \quad 0000 \quad 0000 \quad 0000$$
$$l^{'} = 1011 \quad 0011 \quad 0110 \quad 0011 \quad 1000 \quad 0100 \quad 0101 \quad 0110$$
$$F^{'} = 1011 \quad 0111 \quad 0110 \quad 0011 \quad 1000 \quad 0100 \quad 0101 \quad 0110$$

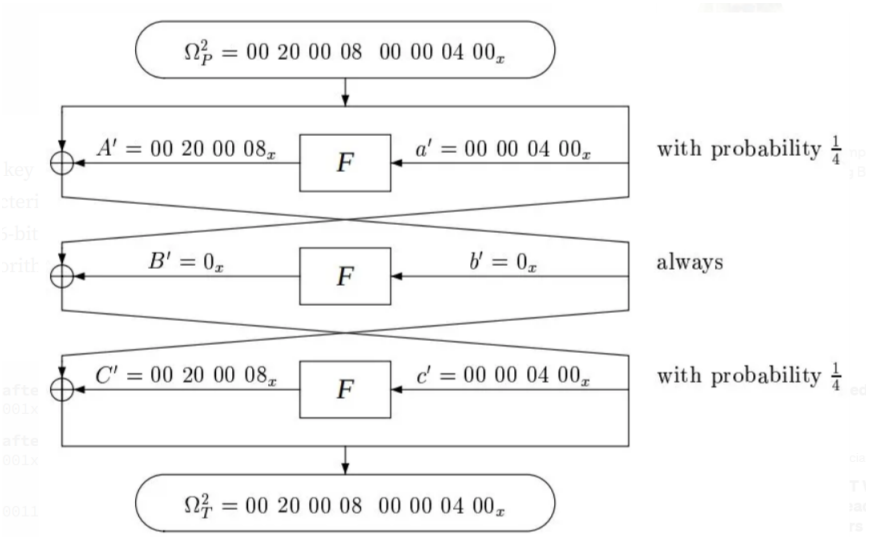
خروجی :S-box
$$1100 \quad 1101 \quad 0100 \quad 0100 \quad 0100 \quad 1101 \quad 0001 \quad 1011$$

برای S۲، جفت ورودی داده شده تعداد کلیدهای '011011', '011101', '111011', and '111101'. را افزایش می دهد برای مثال برای کلید «۰۱۱۰۱۱» (همه مقادیر در کادر زیر فقط مربوط به S۲ هستند). E(f۱)[S۲] نشان دهنده ورودی S۲ در دور ششم است.

$$E(f)[S2] \oplus 011011 = 110100 \oplus 011011 = 101111$$
$$E(f)[S2] \oplus 011011 = 010010 \oplus 011011 = 001001$$
$$S2(101111) = 0010$$
$$S2(001001) = 1111$$
خروجی S-box ۲ $0010 \oplus 1111 = 1101$

با تجزیه و تحلیل ۲۵۰ جفت ورودی، بیت های کلید زیر مربوط به ۵ مورد از جعبه های S را دریافت می کنیم.

$S2 : 111101$
$S5 : 011010$
$S6 : 101100$
$S7 : 111011$
$S8 : 010011$



شکل ۶: مشخصه دوم

با استفاده از مشخصه دوم تجزیه و تحلیل می کنیم:

$S1 : 110010$
$S2 : 111101$
$S4 : 100110$
$S5 : 011010$
$S6 : 101100$

مقادیر کلید محاسبه شده مربوط به S۶ S۵، S۲، باید با استفاده از هر دو ویژگی یکسان باشند. در غیر این صورت جفت ورودی بیشتری را تحلیل کنید. اکنون ۴۲ بیت از کلید ۵۶ بیتی داریم. موقعیت آنها را می توان با استفاده از یک الگوریتم زمان بندی کلیدی تعیین کرد. ۱۴ بیت باقی مانده از کلیدها را می توان با استفاده از بروس فورس پیدا کرد.

کلید پیشنهادی بعد از تجزیه دو مولف
$x11011xxx011001x0xx1011xx10x111xx01xx10x01x1011x11x1000xx001x01x$
کلید بعد از روش بروس فورس برای ۱۴ بیت باقی مانده
$1110111x0011001x0111011x1101111x0011010x0101011x1111000x0001001x$
کلید اصلی
11101111001100110111011011011110001101000101011111110001000100 11

۴ با شکسته شدن الگوریتم DES ،در سال ۲۰۰۱ الگوریتم AES به عنوان استاندارد رمزنگاری انتخاب شد.در مورد نحوه این انتخاب، ساختار و چگونگی کارکرد این الگوریتم تحقیق کنید؟

AES یا همان STANDARD ENCRYPTION ADVANCED مانند DES هردو SYMMETRIC CIPHER BLOCK هستند. DES به خاطر داشتن SIZE KEY کوچمتر مشکل امنیتی داشت. به خاطر همین AES معرفی شد. مسابقات گوناگونی در سال های مختلف در سال های مختلف برای شکستن DES برگزار شد. در سال ۱۹۹۷ در CONTENT I DES با یک حمله BRUTE-FORCE با صرف ۸۴ روز الگوریتم شکسته شد. در سال ۱۱۹۸ هم دو مسابقه برگزار شد در اولین مسابقه حدود یکماه صرف شکستن الگوریتم شد و جمله DICIPHER شده HANDS MANY : IS MESSAGE UNKNOWN "THE WORK" LIGHT MAKE بود. دومین مسابقه هم کمتر از سه روز طول کشید و متن مسابقه "ITS THOSE FOR TIME ۱۲۸-۱۹۲-، AND-BIT ۲۵۶ "،KEYS بود. اخرین مسابقه هم در سال ۱۹۹۹ بود که فقط ۲۲ ساعت و ۱۵ دقیقه طول کشید و به همه ثابت کرد که وقت جایگزین شدن DES فرا رسیده. در سال ۲۰۰۱ در استاندارد FIPS۱۹۷ در الگوریتم AES معرفی شد. در الگوریتم AES حق انتخاب بین کلید های ۲۵۶و۱۹۲-۱۲۸ وجود دارد مشخص است که از کلید های ۵۶ بیتی DES قدرت بیشتری دارد. DES از شبکه فایستل برای تقسیم کلید خود به دو قسمت استفاده کیکرد ولی در AES با استفاده از کل دیتا به عنوان یک تک ماتریس برخورد می شود.
AES: . شامل ۱۶ راند بود DES

۱: برای کلید های ۱۲۸ بیتی شامل ۱۰ راند
۲: برای کلید های ۱۹۲ بیتی شامل ۱۲ راند
۳: برای کلید های ۲۵۶ بیتی شامل ۱۴ راند

این الگوریتم شامل مراحل زیر است:

Subbytes : برای جایگزینی بایت های کل بلاک S-box استفاده از
Rows Shift : matrix جا به جایی ردیف های
Columns: Mix جا به جایی ستون ها
round Add بلاک:keys و کلید انجام میشود . XOR در این مرحله

۵ رمز نگاری یا رمز گشایی یک پیام در الگوریتم AES به زبان پایتون

در نوت بوک

۶ نحوه رمزنگاری AES

در روش رمزنگاری AES اندازه کلید شامل ۱۲۸، ۱۹۲ و ۲۵۶ بیت می‌شود. الگوریتم AES بدون در نظر گرفتن اینکه طول کلید شما ۱۲۸، ۱۹۲ و ۲۵۶ بیت باشد ، دارای یک اندازه بلوک ثابت ۱۲۸ بیتی است. در رمزنگاریAES-128 برای رمزگذاری و رمزگشایی یک پیام از طول کلید ۱۲۸ بیتی استفاده می‌شود، در حالی‌که AES-192 از طول کلید ۱۹۲ بیتی و AES-256 از طول کلید ۲۵۶ بیتی برای این کار بهره می‌برد. اطلاعات به صورت کلی در سه دسته طبقه‌بندی می‌شوند: محرمانه، مخفی یا فوق سری. از تمام طول کلیدها می‌توان برای محافظت از سطح محرمانه و سطح مخفی استفاده کرد. اما اطلاعات فوق سری به طول کلیدهای ۱۹۲ یا ۲۵۶ بیتی نیاز دارد.

برای کلیدهای ۱۲۸ بیتی ۱۰ دور، برای کلیدهای ۱۹۲ بیتی ۱۲ دور و برای کلیدهای ۲۵۶ بیتی ۱۴ دور وجود دارد. یک دور شامل چندین مرحله پردازش است که شامل جایگزینی، جابجایی و ترکیب کردن متن ساده‌ای است که وارد می‌شود و در انتها به متن رمزنگاری شده که خروجی نهایی می‌باشد، تبدیل می‌گردد که قابلیت خواندن آن تنها با کلید خصوصی وجود خواهد داشت. اولین تغییر در رمزگذاری AES نسبت به ورژن قبلی خودش، جایگزینی داده‌ها با استفاده از جدول جایگزینی است. سپس ردیف‌های داده را تغییر می‌دهد و درنهایت ستون‌ها را مخلوط می‌کند. این مراحل امکان نفوذ و هک را به صورت قابل توجهی غیر ممکن می‌کنند.