Kryptering 1 Hösten 2023

Inlämningsuppgift 2

Instruktioner

Denna inlämningsuppgift är ett obligatoriskt examinationsmoment om du är registrerad på kursen MA1489. Om du är däremot är registrerad på MA1490 är inlämningsuppgiften frivillig. Inlämningsuppgiften är värd 2 högskolepoäng, vilket i arbetstid motsvarar ungefär 50 timmar. Betygskalan är G/U. För betyget G krävs att

- svar och lösningar redovisas enskilt (det är tillåtet att samarbeta i grupp och som vanligt är plagiering **inte** tillåtet)
- alla 11 uppgifterna i nästa avsnitt är korrekt lösta
- svar och lösningar lämnas in via Canvas senast **7 januari 2024**.

Uppgifter

Temat på denna inlämningsuppgift är *differentiell kryptoanalys*. Du ska lösa uppgifter som steg för steg beskriver grunderna i differentiell kryptoanalys genom att utgå från Simplified DES som exempel. För information om kryptosystemet se dokumentet *Simplified DES – en lättsmält version av DES*, som du hittar på kursens sida i Canvas.

1. Vi inleder med att bestämma några personliga parametrar, som kommer att användas i kommande uppgifter. Låt $\mathcal{Y}$, $\mathcal{M}$ och $\mathcal{D}$ vara det år, månad respektive dag som du föddes, d v s

$$1899 \leq \mathcal{Y} \leq 2022, \quad 1 \leq \mathcal{M} \leq 12 \quad \text{och} \quad 1 \leq \mathcal{D} \leq 31.$$

Tag $X, Y \in \mathbb{Z}_{16}$, $K \in \mathbb{Z}_{1024}$ och $m \in \mathbb{Z}_{256}$ sådana att

$$\begin{aligned} X &\equiv 5\mathcal{M} + 7\mathcal{D} + 11 \pmod{16}, \\ Y &\equiv 3\mathcal{M} - 9\mathcal{D} + 13 \pmod{16}, \\ K &\equiv \mathcal{Y}\mathcal{M} - \mathcal{D} \pmod{1024} \end{aligned}$$

och

$$m \equiv \mathcal{Y}\mathcal{D} + \mathcal{M} \pmod{256}.$$

Bestäm den binära representation av X, Y, K och m på följande format.

- Elementen i $\mathbb{Z}_{16}$ skrivs med fyra bitar enligt

$$0_{10} = 0000_2,\ 1_{10} = 0001_2,\ 2_{10} = 0010_2,\ \ldots,\ 15_{10} = 1111_2.$$

- Elementen i $\mathbb{Z}_{256}$ skrivs med åtta bitar enligt

$$0_{10} = 00000000_2,\ 1_{10} = 00000001_2,\ \ldots,\ 255_{10} = 11111111_2.$$

- Elementen i $\mathbb{Z}_{1024}$ skrivs med tio bitar på samma sätt som ovan.

I följande två uppgifter används dessa värden på X, Y, K och m. Därefter används de endast om det uttryckligen anges, d v s i övriga uppgifter nollställs X, Y, K och m med undantag i vissa uppgifter..

2. Baserat på K bestäm rundnycklarna K_1 och K_2.

3. Kryptera klartexten m med K som nyckel.

Differentiell kryptoanalys är en valbar klartext-attack, d v s man har möjligt att välja klartexter och kryptera dessa, för att med hjälp av de erhållna kryptogrammen försöka utröna information om rundnycklarna K_1 och K_2.

I uppgift 4–11 antar vi att vi inte vet vilken krypteringsnyckel K som används.

4. Antag att vi valt en klartext m. Låt $(L_0, R_0) = \mathrm{IP}(m)$ och $c = E_K(m)$.

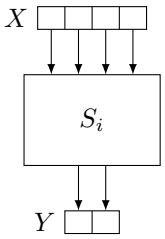
(a) Vilka bitar i m måste sättas lika med 0 för att $L_0 = 0000$ ska gälla?

(b) Antag att vänsterblocket L_0 uppfyller $L_0 = 0000$. Vilka bitar i kryptogrammet c avslöjar utdata från funktionen f_1?

Man kan även välja klartexter så att $R_0 = 0000$ och då med vetskap om motsvarande kryptogram avslöja utdata från f_2. Det fallet behöver du inte utreda. I fortsättning utgår vi från att alla klartexter vi väljer är sådana att $L_0 = 0000$, d v s endast högerblocket R_0 varierar.

5. När vi vet utdata från funktionen f_i vet vi också utdata från S-box S_0 och S_1. Antag att $f_1(R_0, K_1) = Y$, där Y är din personliga parameter från uppgift 1. Bestäm utdata från S_0 och S_1.

Härnäst tittar vi lite närmare på S-box S_0 och S_1.



Låt X och Y vara bitsträngar som betecknar in- respektive utdata från en S-box. Då består X av fyra bitar och Y av två bitar.

6. Låt X vara din personliga parameter från uppgift 1 och $\Delta X = 0101$. Sätt $X' = X \oplus \Delta X$.

(a) Bestäm utdata Y och Y' från S_i med X respektive X' som indata, där $i \in \mathbb{Z}_2$ sådant att $i \equiv \mathcal{D} \pmod 2$.

(b) Bestäm $\Delta Y = Y \oplus Y'$.

Bitsträngen ΔX beskriver skillnaden mellan X och X' på så sätt att på de positioner i ΔX där biten är lika med 1 är X och X' olika och på de positioner i ΔX där biten är lika med 0 är X och X' lika. Detsamma gäller ΔY kontra Y och Y'.

Tabell 1 visar hur många par X och X' sådana att $\Delta X = X \oplus X'$ och som vars motsvarande utdata från S_0 respektive S_1 ger $\Delta Y = Y \oplus Y'$. Enligt tabell 1 finns det tio par (X, X') med differensen $\Delta X = 0111$ vilka ger differensen $\Delta Y = 10$ när man använder S-boxen S_0. Det går att bilda 16 par (X, X') som har samma differens ΔX. Med andra ord är sannolikheten att vi får karakteristiken $(\Delta X, \Delta Y) = (0111, 10)$ lika med $10/16 = 5/8$.

Då $\Delta X = 0000$ är $X = X'$ och därmed $Y = Y'$, d v s $\Delta Y = 00$. Man kan uttrycka det som ”ingen skillnad in ger ingen skillnad ut”. Det är anledningen till att första raden i tabellerna har värdena $16, 0, 0, 0$. I fortsättningen bortser vi från denna rad.

7. Vilken karakteristik $(\Delta X^*, \Delta Y^*)$ för S_0 har störst sannolikhet? Tänk på att du ska bortse från den ointressanta karakteristiken $(0000, 00)$.

	ΔY			
ΔX	00	01	10	11
0000	16	0	0	0
0001	0	2	10	4
0010	0	10	6	0
0011	2	4	0	10
0100	2	4	8	2
0101	10	0	4	2
0110	0	2	2	12
0111	4	10	2	0
1000	2	4	8	2
1001	8	2	2	4
1010	4	2	2	8
1011	2	8	4	2
1100	8	2	2	4
1101	2	4	8	2
1110	2	8	4	2
1111	4	2	2	8

	ΔY			
ΔX	00	01	10	11
0000	16	0	0	0
0001	2	8	2	4
0010	0	6	4	6
0011	4	2	8	2
0100	2	0	10	4
0101	2	4	2	8
0110	0	10	0	6
0111	8	2	4	2
1000	4	6	0	6
1001	8	2	4	2
1010	2	0	10	4
1011	0	6	4	6
1100	0	6	4	6
1101	6	0	6	4
1110	10	4	2	0
1111	2	8	2	4

Tabell 1. Fördelning av differenser i S_0 respektive S_1.

8. Förklara varför ΔX inte påverkas av nyckeladditionen inne i f_1 innan S-boxen? Här betecknar ΔX differensen mellan två indata till S-boxen.

9. Med utgångspunkt från den karakteristik du fann i uppgift 7 vilka bitar i R_0 och R'_0 ska vara olika och vilka bitar ska vara lika så att de ger ΔX^*?

10. Baserat på föregående uppgift sätt $\Delta R_0^* = R_0 \oplus R'_0$. Vilka bitar i klartexten m och m' ska vara olika så att de efter IP ger differensen ΔR_0^*?

11. Vidare vilka bitar i motsvarande kryptogram c och c' hör till ΔY^*? Här betecknar ΔY^* differensen mellan två utdata från S-boxen.

Differentiell kryptoanalys av de bitar i rundnyckeln K_1, d v s de fyra första bitarna, som påverkar S_0 går nu till på följande sätt.

Välj flera par av klartexter (m, m') sådana att de ger differensen ΔR_0^* efter IP.
Kryptera varje (m, m') till motsvarande par av kryptogram (c, c').
Nollställ en räknare för varje möjlig delnyckel (2^4 stycken).
För varje möjlig delnyckel $K_{1,0} = (k_{1,0}k_{1,1}k_{1,2}k_{1,3})$:
    För varje $(m, m') \mapsto (c, c')$:
        Följ bitarna i c och c' bakåt till motsvarande utdata Y respektive Y' från S_0.
        Om $Y \oplus Y' = \Delta Y^*$:
            Kryptera R_0 och R'_0 med $K_{1,0}$ till och med S_0. Beteckna resultaten Z och Z'.
            Om $Z \oplus Z' = \Delta Y^*$:
                Öka räknaren för $K_{1,0}$ med 1.

Den delnyckel vars räknare är störst antas motsvara de fyra första bitarna i rundnyckeln K_1. Genom att istället välja en karakteristik för S_1 med hög sannolikhet kan följa bitar från kryptogram c till S_1 och på så sätt knäcka de fyra sista bitarna i rundnyckeln K_1. Tänk på att man måste välja andra par (m, m') av klartexter.

Notera att metoden måste anpassas för varje kryptosystem och Simplified DES är ett alltför enkelt kryptosystem för att fullt ut visa hur differentiell kryptoanalys går till.