Дискрет мат, Семинар №11

1. $p = 19$, $q = 29$ үед $n = pq$ гэе. $\varphi(n) =?$, $e = 11$ үед $d =?$ ол. RSA алгоритмаар $m = 5$ тоог илгээхэд ямар тоо хүлээн авах вэ?

Бодолт 1.

Заавар:

Бодолт: $n = 19 \cdot 29 = 551$, $\varphi(19 \cdot 29) = (19-1)(29-1) = 18 \cdot 28 = 504$,

$$e \cdot d \equiv 11d \equiv 1 \pmod{504} \Rightarrow 11d - 504m = 1$$

$11x - 504y = 1$ тэгшитгэлийн бүхэл шийдийг Эвклидийн алгоритм ашиглан бодъё.
$504 = 11 \cdot 45 + 9$, $11 = 9 + 2$ $9 = 2 \cdot 4 + 1$ тул

$$\begin{aligned} 1 &= 9 - 2 \cdot 4 \\ &= 9 - (11 - 9) \cdot 4 = 9 \cdot 5 - 11 \cdot 4 \\ &= (504 - 11 \cdot 45) \cdot 5 - 11 \cdot 4 \\ &= 504 \cdot 5 - 11 \cdot 229 = 11 \cdot (-229) - 504 \cdot (-5) \end{aligned}$$

тул $d \equiv -229 \equiv 275 \pmod{504}$ буюу $d = 275$ боллоо. $m = 5$ тоог

$$5^{11} \equiv 158 \pmod{551}$$

гэж хүлээн авна.

2. RSA-д $p = 11$, $q = 17$, $e = 59$ гэе. d хэдтэй тэнцүү байх вэ? Хэрвээ 111 гэсэн тоог хүлээн авсан бол ямар тоо илгээсэн вэ?

Бодолт 1.

Заавар: $d = 19$, 100

Бодолт:

3. RSA-д $p = 7$, $q = 19$, $e = 25$ гэе. d хэдтэй тэнцүү байх вэ? Хэрвээ хүлээн авсан тоо 43 бол ямар тоо илгээсэн бэ?

Бодолт 1.

Заавар: $d = 13$, 36

Бодолт:

4. RSA-д $p = 11$, $q = 31$, $e = 131$ гэе. d хэдтэй тэнцүү байх вэ? Хэрвээ 100 гэсэн илгээсэн бол ямар тоо хүлээн авах вэ?

Бодолт 1.

Заавар: $d = 71$, 144

Бодолт:

5. RSA-д $p = 19, q = 23, e = 31$ бол d-г ол. 56-г ямар тоо болгон илгээх вэ? Гарсан тооноос хэрхэн 56-г гарган авах вэ?

Бодолт 1.

Заавар:

Бодолт: $(p-1)(q-1) = (11-1)(19-1) = 180$ байна. Түүнчлэн

$$7x - 180y = 1$$

тэгшитгэлийн Эвклидийн алгоритм ашиглан бодвол

$$\begin{aligned} 180 &= 25 \cdot 7 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

тул

$$\begin{aligned} 1 &= 1 \times 5 - 2 \times 2 \\ &= 1 \times 5 - 2 \times () \end{aligned}$$

Иймд ерөнхий шийд нь

$$\begin{cases} x = -77 + 180n \\ y = -3 + 7n \end{cases}$$

байна. Эндээс $x \in \mathbb{Z}_{180}$ гэвэл $n = 1$ үед $x = -77 + 180 \cdot 1 = 103$ болно. Иймд $d = 103$. $11 \cdot 19 = 209$ ба

$$100^7 \equiv 111 \pmod{209}$$

тул 100 гэсэн мессежийг 111 болгон илгээнэ. Харин ирсэн 111 мессежийг

$$111^{103} \equiv 100 \pmod{209}$$

гэж буцаана.

6. 10100111, 11010011 код үгүүдийн Хэммингийн зайг ол.

7. Аль ч хоёр код үгийнх нь Хэммингийн зай нь дор хаяж 7 байдаг кодоор ямар алдааг засаж болох вэ?

8. $C \subseteq \{0,1\}^{10}$ код нь 2 алдаа засдаг байг. $|C| \leq 18$ болохыг харуул.

9. $C \subseteq \{0,1\}^{15}$ код нь 3 алдаа засдаг байг. $|C| \leq 56$ болохыг харуул.

10. $n = 5$ үед 1 алдаа залруулдаг код хэрхэн үүсгэх вэ? Энэ кодоор $a = 11010$-г дамжуулахад 6-р оронд алдаа гарсан бол алдааг хэрхэн залруулах вэ?

Бодолт 1.

Заавар:

Бодолт: $2^5 \leq \dfrac{2^m}{m+1}$ байх хамгийн бага m тоог олъё. $m = 6$, $m = 7$, $m = 8$ утгуудыг шалгавал $32 > \dfrac{64}{7}$, $32 > \dfrac{128}{8} = 16$, $32 > \dfrac{256}{9}$ ба $m = 9$ үед $32 < \dfrac{512}{10}$ тул $m = 9$, $k = m - n = 4$ байна.
1, 2, 4, 8 нь хяналтын гишүүд, иймд 3, 5, 6, 7, 9 нь мэдээлэгч гишүүд юм. Иймд $\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5$ мэдээллийг кодловол

$$\beta_3 = \alpha_1, \beta_5 = \alpha_2, \beta_6 = \alpha_3, \beta_7 = \alpha_4, \beta_9 = \alpha_5$$

гэсэн мэдээлэгч гишүүд үүснэ. Хяналтын гишүүд нь

$$\begin{aligned}
1 &= 2^0 \\
2 &= 2^1 \\
3 &= 2^0 + 2^1 \\
4 &= 2^2 \\
5 &= 2^0 + 2^2 \\
6 &= 2^1 + 2^2 \\
7 &= 2^0 + 2^1 + 2^2 \\
8 &= 2^3 \\
9 &= 2^0 + 2^3
\end{aligned}$$

тул

$$\begin{aligned}
\beta_1 &= \beta_3 + \beta_5 + \beta_7 = \alpha_1 + \alpha_2 + \alpha_4 \\
\beta_2 &= \beta_3 + \beta_6 + \beta_7 = \alpha_1 + \alpha_3 + \alpha_4 \\
\beta_4 &= \beta_5 + \beta_6 + \beta_7 = \alpha_2 + \alpha_3 + \alpha_4 \\
\beta_8 &= \beta_9 = \alpha_5
\end{aligned}$$

болно. Иймд $a = 11010$ код үгийг $\beta_1 = 1+1+1 = 1$, $\beta_2 = 1+0+1 = 0$, $\beta_3 = 1$, $\beta_4 = 1+0+1 = 0$, $\beta_5 = 1$, $\beta_6 = 0$, $\beta_7 = 1$, $\beta_8 = 0$, $\beta_9 = 0$ буюу 101010100 гэж кодлоно. Дамжуулахад 6-р оронд алдаа гарсан бол 101011100 мэдээллийг хүлээн авах β_6 орсон хяналтын гишүүд дээр алдаа гарсан байх ёстой. Үнэхээр

$$0 = \beta_2 \neq \beta_3 + \beta_6 + \beta_7 = 1 + 1 + 1 = 1$$

$$0 = \beta_4 \neq \beta_5 + \beta_6 + \beta_7 = 1 + 1 + 1 = 1$$

байна. Эндээс алдаа гарсан цифрийг $2 + 4 = 6$ гэж олоод $101011100 \to 101010100$ гэж сэргээнэ. Мэдээлэгч гишүүд нь 3, 5, 6, 7, 9 тул анхны мэдээг $\beta_3\beta_5\beta_6\beta_7\beta_9 = 11010$ гэж сэргээж уншина.