

**현대암호학기초**

**RSA 이용한 디지털 서명**

2018111337 송희원

[9조] 송희원, 권혜민, 윤명지, 이현정

**평문** = I give you 100000000 won N=2501 <2501<이므로 11비트씩 쪼갠다.

***[서명 생성 과정]***

**1) 평문을 16진수로 바꾼다.**

Igiveyou100000000won

49 67 69 76 65 79 6F 75 31 30 30 30 30 30 30 30 30 77 6F 6E

**2) 16진수를 2진수로 바꾼다.**

0100 1001 0110 0111 0110 1001 0111 0110 0110 0101 0111 1001 0110 1111 0111 0101 0011 0001 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0111 0111 0110 1111 0110 1110

**3) 11비트씩 쪼갠다**

0100 1001 011/0 0111 0110 10/01 0111 0110 0/110 0101 0111/ 1001 0110 111/1 0111 0101 00/11 0001 0011 0/000 0011 0000/ 0011 0000 001/1 0000 0011 00/00 0011 0000 0/011 0000 0011 /0000 0111 011/1 0110 1111 01/10 1110(padding00000)

**4) 쪼갠 비트를 10진수로 바꾼다**

0100 1001 011/0 0111 0110 10/01 0111 0110 0/110 0101 0111/ 1001 0110 111/1 0111 0101 00/11 0001 0011 0/000 0011 0000/ 0011 0000 001/1 0000 0011 00/00 0011 0000 0/011 0000 0011 /0000 0111 011/1 0110 1111 01/10 1110(padding00000)

↓

587 474 748 1623 1207 1492 1572 48 387 1036 96 777 59 1469 1241

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 587 | 474 | 748 | 1623 | 1207 | 1492 | 1572 | 48 | 387 | 1036 | 96 | 777 | 59 | 1469 | 1241 |
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| 1060 | 1294 | 1855 | 1793 | 2027 | 2107 | 1965 | 1539 | 1740 | 304 | 612 | 1683 | 1002 | 675 | 1862 |

**5) 서명 값 구하기 ( 서명 값 = )**

// 첫번째 줄은 메시지를 의미함.

// ↓의 의미는 위의 숫자에 11계승(D)을 한 후 모드 2501(N)을 취한 값이 아래 숫자라는 것

// 세번째 줄은 서명 값을 의미함

∴ 서명 값은

1060 1294 1855 1793 2027 2107 1965 1539 1740 304 612 1683 1002 675 1862

***[서명 검증 과정]***

**1) 메시지 값 구하기 ( )**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1060 | 1294 | 1855 | 1793 | 2027 | 2107 | 1965 | 1539 | 1740 | 304 | 612 | 1683 | 1002 | 675 | 1862 |
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| 587 | 474 | 748 | 1623 | 1207 | 1492 | 1572 | 48 | 387 | 1036 | 96 | 777 | 59 | 1469 | 1241 |

// 첫번째 줄은 서명 값을 의미함.

// ↓의 의미는 위의 숫자에 11계승(E)을 한 후 모드 2501(N)을 취한 값이 아래 숫자라는 것

// 세번째 줄은 메시지를 의미함

**2) 메시지를 2진수로 바꾼다**

587 474 748 1623 1207 1492 1572 48 387 1036 96 777 59 1469 1241

↓

0100 1001 011/0 0111 0110 10/01 0111 0110 0/110 0101 0111/ 1001 0110 111/1 0111 0101 00/11 0001 0011 0/000 0011 0000/ 0011 0000 001/1 0000 0011 00/00 0011 0000 0/011 0000 0011 /0000 0111 011/1 0110 1111 01/10 1110(padding00000)

**3) 2진수를 16진수로 바꾼다**

0100 1001 0110 0111 0110 1001 0111 0110 0110 0101 0111 1001 0110 1111 0111 0101 0011 0001 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0011 0000 0111 0111 0110 1111 0110 1110

↓

49 67 69 76 65 79 6F 75 31 30 30 30 30 30 30 30 30 77 6F 6E

**4) 16진수를 평문으로 바꾼다.**

49 67 69 76 65 79 6F 75 31 30 30 30 30 30 30 30 30 77 6F 6E

Igiveyou100000000won

∴ **평문** = I give you 100000000 won