UNIVERSITY OF RAJSHAHI

Rajshahi, BANGLADESH.

Course Code:

ICE 4221

Course Title :

Cryptography and Network security

Introduction to Number Theory

Prime Numbers

- Prime numbers only have divisors of 1 and self
  - they cannot be written as a product of other numbers
  - note: 1 is prime, but is generally not of interest
- eg. 2,3,5,7 are prime, 4, 6, 8, 9, 10 are not
- Prime numbers are central to number theory
- List of prime number less than 200 is:

```
2  3  5  7  11  13  17  19  23  29  31  37  41  43  47  53  59  61  67
71  73  79  83  89  97  101  103  107  109  113  127  131  137  139
149  151  157  163  167  173  179  181  191  193  197  199
```

Prime Number

The primes less than 2000

2	101	211	307	401	503	601	701	809	0	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1999
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Prime Factorisation

- To **factor** a number n is to write it as a product of other numbers: $n=a \times b \times c$
- Note that factoring a number is relatively hard compared to multiplying the factors together to generate the number
- The **prime factorisation** of a number n is when its written as a product of primes
  - eg. $91=7\times13$; $3600=2^4\times3^2\times5^2$
  - It is unique

$$a = \prod_{p \in P} p^{a_p}$$

Relatively Prime Numbers & GCD

- Two numbers `a, b` are **relatively prime** if have **no common divisors** apart from 1
    - eg. 8 & 15 are relatively prime since
        - factors of 8 are 1,2,4,8 and
        - Factors of of 15 are 1,3,5,15 and
        - 1 is the only common factor

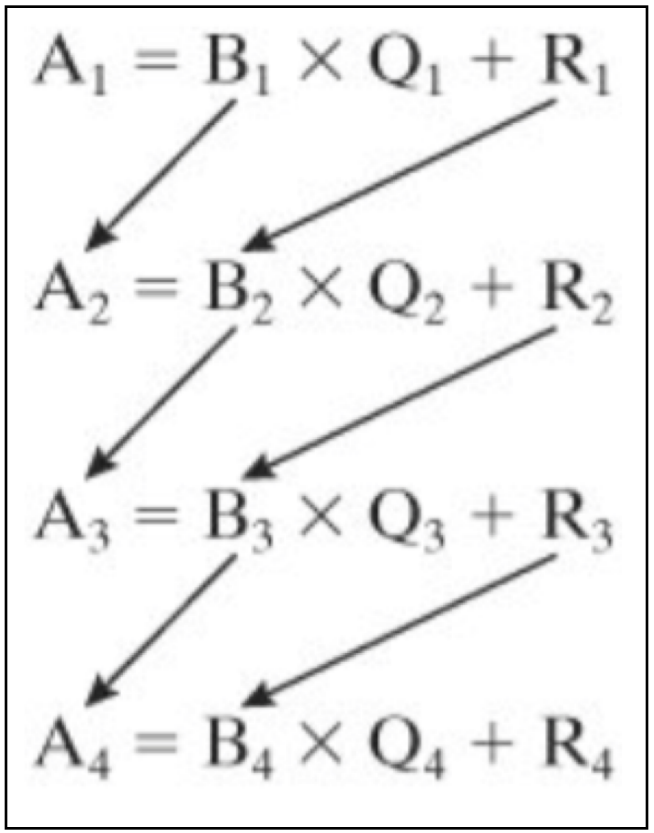
Relatively Prime Numbers & GCD

- Conversely can determine the greatest common divisor by comparing their prime factorizations and using least powers
  - eg. $300=2^1\times3^1\times5^2$ $18=2^1\times3^2$
  - hence $GCD(18,300)=2^1\times3^1\times5^0=6$

The Euclidean Algorithm

It is a simple procedure for determining the greatest common divisor (GCD) of two positive integers.

```
UCLID(a, b)
1.  A ← a; B ← b
2. if B = 0 return A = gcd(a, b)
3. R = A mod B
4. A ← B
5. B ← R
6. goto 2
```



The Euclidean Algorithm

Instant Test:

Find gcd(1970, 1066)

1970	= 1 x 1066 + 904	gcd(1066, 904)
1066	= 1 x 904 + 162	gcd(904, 162)
904	= 5 x 162 + 94	gcd(162, 94)
162	= 1 x 94 + 68	gcd(94, 68)
94	= 1 x 68 + 26	gcd(68, 26)
68	= 2 x 26 + 16	gcd(26, 16)
26	= 1 x 16 + 10	gcd(16, 10)
16	= 1 x 10 + 6	gcd(10, 6)
10	= 1 x 6 + 4	gcd(6, 4)
6	= 1 x 4 + 2	gcd(4, 2)
4	= 2 x 2 + 0	gcd(2, 0)
Therefore, gcd(1970, 1066) = 2		

Multiplicative Inverse:

- If gcd (m,b)=1, then b has a multiplicative inverse modulo *m*
- That is, for positive integer b<m, there exist a b^{-1} such that bb^{-1} =1 mod *m*.
- The Euclidean algorithm can be extended so that, in addition to finding gcd(m,b), if gcd is 1.
- The extended Euclidean algorithm returns the multiplicative inverse of b

Finding Multiplicative Inverse:

Using Extended Euclidean Algorithm

EXTENDED EUCLID (m,b)

1. **(A1, A2, A3) ← (1, 0, m); (B1, B2, B3) ← (0,1, b)**
2. **If B3 = 0 return A3 = gcd(m, b); no inverse.**
3. **If B3 = 1 return B3 = gcd (m, b); B2 = b^{-1} mod m**
4. **Q= [A3 / B3]**
5. **(T1, T2, T3) ← (A1 - QB1, A2 – QB2, A3-QB3)**
6. **(A1, A2, A3) ← (B1, B2, B3)**
7. **(B1, B2, B3) ← (T1, T2, T3)**
8. **goto 2**

Finding Multiplicative Inverse of 550 in GF (1759)

Using Extended Euclidean Algorithm

Q	A1	A2	A3	B1	B2	B3
	1	0	1759	0	1	550
3	0	1	550	1	-3	109
5	1	-3	109	-5	16	5
21	-5	16	5	106	-339	4
1	106	-339	4	-111	355	1

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = GCD(m, b); no inverse
3. if B3 = 1
   return B3 = GCD(m, b); B2 = b^-1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 - Q B1, A2 - Q B2, A3 - Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

Fermat's Theorems

Two theorems that play important roles in public-key cryptography are Fermat's theorem and Euler's theorem.

Fermat's Theorem:

Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 \ (mod\ p)$$

Example: **Instantly considered**

An alternative form of Fermat's theorem is also useful: If p is prime and a is a positive integer, then

$$a^{p} \equiv a \ (mod\ p)$$

Example: **Instantly considered**

First form of the theorem requires that b be relatively prime to P, but this form does not.

[**Proof of Fermat's theorem should be self studied**]

Euler's Totient Function

Euler's Totient Function, f(n), defined as the number of positive integers less than n and relatively prime to n. By convention, f(1) = 1.

Example:

Determine $\phi(37)$ and $\phi(35)$.

Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus $\phi(37) = 36$.

To determine $\phi(35)$, we list all of the positive integers less than 35 that are relatively prime to it:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18,

19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

There are 24 numbers on the list, so $\phi(35) = 24$.

Instant Exercise:

Euler's Totient Function (Cont')

✓It should be clear that for a prime number p,

$$\varphi(p) = p - 1$$

✓Now suppose that we have two prime numbers p and q, with $p \neq q$. Then we can show that for n= pq

$$\varphi(n) = \varphi(\mathrm{pq}) = \varphi(p) \times \varphi(q) = (p-1) \times (q-1)$$

Euler's Totient Function (Cont')

Table 8.2 Some Values of Euler's Totient Function $\phi(n)$

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

Prove that Ø(20) is 8.

Euler's Theorem

Euler's theorem states that for every a and n that are relatively prime:

$$a^{\varphi(n)} \equiv 1 (mod\ n)$$

Example: Instant Considered.

$a = 3; n = 10; \phi(10) = 4$	$a^{\phi(n)} = 3^4 = 81 \equiv 1 (\text{mod } 10) = 1 (\text{mod } n)$
$a = 2; n = 11; \phi(11) = 10$	$a^{\phi(n)} = 2^{10} = 1024 \equiv 1 (\text{mod } 11) = 1 (\text{mod } n)$

The Powers of an Integer, Modulo n

Euler's theorem states that for every a and n that are relatively prime:

$$a^{\varphi(n)} \equiv 1 (mod\ n)$$

where $\varphi(n)$, Eular's totient function, is the number of positive integers less than n and relatively prime to n

Primitive Root

More generally, we can say that the highest possible exponent to which a number can belong (mod n) is $\varphi(n)$. If a number is of this order, it is referred to as a **primitive root** of n.

The importance of this notion is that if a is a primitive root of n, then its powers
a, a^2,..., $a^{\varphi(n)}$ are distinct (mod n) and are all relatively prime to n.

In particular, for a prime number p, if a is a primitive root of p, then a, a^2,..., a^{p1} are distinct (mod p).

For the prime number 19, its primitive roots are 2, 3, 10, 13, 14, and 15.

Primitive Root

- Let n be a prime integer.
- Then, g is a primitive root for n if the first n-1 powers of g: $g^1, g^2, g3, \ldots\ldots g^{n-1}$ include all of the distinct n-1 integers (except 0) in the class modulo n.
  - For example: 3 is a primitive root of 7.

$$
\begin{aligned}
3^1 &= 3 = 3^0 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7 \\
3^2 &= 9 = 3^1 \times 3 \equiv 3 \times 3 = 9 \equiv 2 \pmod 7 \\
3^3 &= 27 = 3^2 \times 3 \equiv 2 \times 3 = 6 \equiv 6 \pmod 7 \\
3^4 &= 81 = 3^3 \times 3 \equiv 6 \times 3 = 18 \equiv 4 \pmod 7 \\
3^5 &= 243 = 3^4 \times 3 \equiv 4 \times 3 = 12 \equiv 5 \pmod 7 \\
3^6 &= 729 = 3^5 \times 3 \equiv 5 \times 3 = 15 \equiv 1 \pmod 7
\end{aligned}
$$

Note: A prime integer could have one or more primitive roots.

Primitive Root

Table 8.3 Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

For the prime number 19, its primitive roots are 2, 3, 10, 13, 14, and 15.

Discrete Logarithm

- In general, the goal of exponentials is to calculate the product:

For example: $\mathbf{x=2^3}$

- The goal of logarithms is to calculate the exponents:

For example: $\mathbf{x= \log_2(8) \quad (8=2^x)}$

- The discrete logarithm, we need to apply a modulo operation in the letter:
  - $\mathbf{x= \log_2 8 \pmod{13}}$
- Other way of notation $\mathbf{x = d\log_{2,13}(8)}$
  - Equivalently, $\mathbf{8=2^x \pmod{13}}$

Where: x=exponent, 2=base, 13= modulus, 8 remainder.

Discrete Logarithm

- Example :
  - **2^x (mod 7) = 4** **[we need to find the value of x]**
    - **x= 2 or 5 x={1….6}**
    - **4 (mod 7) = 4 and 32 (mod 7) = 5**
- There are two solutions. In the world of cryptography we are interested in discrete logarithms where each exponent has a distinct remainder.
- If seems that if the modulus (p) of a prime number there are certain base values (b) which generate distinct remainders for different exponents (x= 1. 2, p-1).

Discrete Logarithm

- Example :

• Lets calculate $b^x \pmod 7$ = remainder $x = \{1,\ldots,6\}$ modulus $p = 7$

b	$b^1 \bmod 7$	$b^2 \bmod 7$	$b^3 \bmod 7$	$b^4 \bmod 7$	$b^5 \bmod 7$	$b^6 \bmod 7$
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	**3**	**2**	**6**	**4**	**5**	**1**
4	4	2	1	4	2	1
5	**5**	**4**	**6**	**2**	**3**	**1**
6	6	1	6	1	1	1

- **The discrete logarithm for modulus 7 generate distinct remainders when using base value 3 or 5 and the remainder are in the range {1, ……, 6}**

Discrete Logarithm

- The base value 3 and 5 are called the primitive roots of 7 or generators, often indicated by symbol α .
- It is called generator because applying the multiplication operation on single element (α^x), generates all elements in the discrete value (1….p-1).
- The word discrete in discrete logarithm refer to the aspect that we are working in a distinct group {1…p-1}.

Discrete Logarithm

- Calculating $3^{11} \bmod 7 = x$ is very easy.
- But doing the opposite, calculating the discrete logarithm **$11 = 3^x \bmod 17$** is very difficult. Especially if the modulus is ***at least 309 digits long***.
- **REMEMBER**: Calculating a discrete logarithm is HARD.
- To solve $11 = 3^x \bmod 17$ a computer need to try each exponent x= 1,2,3,4 until the equation matches.

Discrete Logarithm

- In the previous example (p=11) the cyclic group referred to with : Z^*p.
- For example: Z^*p
  - The * means no zero
  - The discrete group is {1, 2, …., p-1}= 10.
  - The number of element in the discrete group is p-1.
- Cyclic group are the basis of discrete logarithm crypto systems

Discrete Logarithm

- Example: α (generator) = 2 and p (modulus) = 11 discrete group {1, …, p -1}

$2^1 \bmod 11 = 2$	$2^6 \bmod 11 = 9$	$2^{11} \bmod 11 = 2$	$2^{16} \bmod 11 = 9$
$2^2 \bmod 11 = 4$	$2^7 \bmod 11 = 7$	$2^{12} \bmod 11 = 4$	$2^{17} \bmod 11 = 7$
$2^3 \bmod 11 = 8$	$2^8 \bmod 11 = 3$	$2^{13} \bmod 11 = 8$	$2^{18} \bmod 11 = 3$
$2^4 \bmod 11 = 5$	$2^9 \bmod 11 = 6$	$2^{14} \bmod 11 = 5$	$2^{19} \bmod 11 = 6$
$2^5 \bmod 11 = 10$	$2^{10} \bmod 11 = 1$	$2^{15} \bmod 11 = 10$	$2^{20} \bmod 11 = 1$

- This is called a cyclic group of generator α , after a certain number of exponentials and modulus operations , we have loop.
- If the remainder ha value 1, the cycle starts all over again in the same order.

Discrete Logarithm

Table 8.3 Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Discrete Logarithm

Table 8.4 Tables of Discrete Logarithms, Modulo 19

(a) Discrete logarithms to the base 2, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(b) Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(c) Discrete logarithms to the base 10, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

(d) Discrete logarithms to the base 13, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(e) Discrete logarithms to the base 14, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9

(f) Discrete logarithms to the base 15, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

Test for Primality

Let n is given. Check whether n is composite or prime number

Miller-Rabin Algorithm

- Step-1: $n-1= m \times a^k$
- Step -2: $T= a^m \bmod n$; $1<a<n-1$
- Step-3: for (p=1 to k-1)

```
{
   T=T^2 mod n
        if (T=+1)
           return (composite)
        if (T=-1)
           return prime
}
```

If k=1 then n is composite number