# CMPE-552 Database and File Security

# Problem Session 23.12.2019

Cryptography, both symmetric and asymmetric, widely uses number theory, in particular, relative primality, modular arithmetics, and multiplicative inverses. That’s why we begin with them.

1. Primality, Greatest Common Divisor (GCD), Euclidean Algorithm

Prime number is one having no other factors except one and itself, e.g. N=7 is a prime number

Relatively prime are such two numbers that have no common factors except one

Greatest Common Divisor (GCD) is the maximal common factor for two numbers

For example, gcd(12,15)=3

GCD can be obtained by factoring the numbers and comparing them

For example, 12=2x2x3, 15=3x5, hence, gcd(12,15)=3

Euclidean algorithm provides straightforward method of finding gcd without necessity of finding factors

EUCLID(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 algorithm has the following progression:

A1=B1xQ1+R1

A2=B2xQ2+R2

A3=B3xQ3+R3

*To find gcd(1970,1066)*

*1970=1x1066+904 gcd(1066,904)*

*1066=1x904+162 gcd(904,162)*

*904=5x162+94 gcd(162,94)*

*162=1x94+68 gcd(94,68)*

*94=1x68+26 gcd(68,26)*

*68=2x26+16 gcd(26,16)*

*26=1x16+10 gcd(16,10)*

*16=1x10+6 gcd(10,6)*

*10=1x6+4 gcd(6,4)*

*6=1x4+2 gcd(4,2)*

*4=2x2+0 gcd(2,0)*

*Therefore, gcd(1970,1066)=2*

Given any positive integer n and any integer a, if we divide a by n, we get an integer quotient q and an integer remainder r that obey the following relationship:

a=qn+r 

where  is the largest integer less than or equal to x.



The remainder r is often referred to as a residue. Let Zn ={0,1,..,n-1}.



In general, an integer has a multiplicative inverse in Zn, if that integer is relatively prime to n. Table 4.1c shows that the integers 1, 3, 5, and 7 have a multiplicative inverse, but 2, 4, and 6 do not.



1. Multiplicative inverse, Extended Euclid



If gcd(m,b)=1, then b has a multiplicative inverse modulo m. That is, for positive integer b<m, there exists a b-1<m such that b b-1=1 mod m. Euclid’s algorithm can be extended so that, in addition to finding gcd(m,b), if the gcd is 1, the algorithm returns the multiplicative inverse of b.

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=
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

Throughout the computation, the following relationships hold:

mT1+bT2=T3 mA1+bA2=A3 mB1+bB2=B3

To see that algorithm correctly returns gcd(m,b), note that if we equate A and B in Euclid’s algorithm with A3 and B3 in the extended Euclid’s algorithm, then the treatment of the two variables is identical. Note also that if gcd(m,b)=1, then on the final step we would have B3=0 and A3 =1. Therefore, on the preceding step, B3=1. But if B3=1, then we can say the following:

mB1+bB2=B3

mB1+bB2=1

bB2=1-mB1

bB21 mod m

Hence, B2 is the multiplicative inverse of b.

Table 4.4 is an example of the execution of the algorithm. It shows that gcd(550,1759)=1 and that the multiplicative inverse of 550 is 355; that is, 550x3551 mod 1759.



1. Asymmetric ciphers

Let’s consider RSA algorithm. We define keys for this algorithm and apply encryption-decryption.

1. Select two distinct prime numbers, p, and q. Let p=7, q=17.
2. Calculate N=pq=7x17=119.
3. Calculate  - the number of relatively prime to N numbers, less than N
4. Select e such that e is relatively prime to . For example, e=7. Actually, gcd(96,7)=gcd(7,5)=gcd(5,2)=gcd(2,1)=gcd(1,0)=1
5. Determine d such that (ed) mod  =1. We use Extended Euclid

Initialization:

A=(1,0,96), B=(0,1,7)

It is true that

A1x96+A2x7=A3, B1x96+B2x7=B3

These equalities hold always for Extended Euclid algorithm

Calculate =int(96/7)=13

Calculate T=A-QB:

T1=1; T2=-13;T3=5 => T=(1,-13,5)

Set A=B=(0,1,7)

Set B=T=(1,-13,5)

B3 is not equal to 0, or to 1, and we continue

Calculate =int(7/5)=1

Calculate T=A-QB:

T1=-1; T2=14;T3=2 => T=(-1,14,2)

Set A=B=(1,-13,5)

Set B=T=(-1,14,2)

B3 is not equal to 0, or to 1, and we continue

Calculate =int(5/2)=2

Calculate T=A-QB:

T1=3; T2=-41;T3=1 => T=(3,-41,1)

Set A=B=(-1,14,2)

Set B=T=(3,-41,1)

B3 is equal to 1, and we stop

=B2=-41=-1x96+5555 mod 96

Let’s check that 7x55 mod 96 =1:

7x55 = 385 = 4x96+11 mod 96

Let’s now apply RSA for encryption of some number less than N, for example, M=20:



To decrypt, we calculate





Hence,



Thus, we got the original message M.

To encipher bytes, we need N>255.

1. How asymmetric encryption can be used for secure communication?
2. How asymmetric encryption can be used for establishing session key?
3. What is digital signature? What is hash (digest) function? What is one-way function? What are requirements to hash function?
4. How digital signature can be used to provide non-repudiation?
5. What is the use of S in message M1 in Kerberos?
6. Why message M2 has two items?
7. What is the use of authenticator in Kerberos?
8. What is the use of Ticket Granting Server in Single Sign-On Kerberos?
9. How nonces can be implemented in Kerberos?
10. How session key is established in Secure Sockets Layer protocol?
11. What is the use of cookies in Passport protocol?
12. How money can be sent with PayPal?
13. How messages to a merchant and payment gateway are bound in Secure Electronic Transaction (SET) protocol?
14. How goods atomicity can be provided by SET extension?
15. What is notational money? Token money? What is redundancy predicate? How redundancy predicate is used to verify validness of token money? How denomination of token money is verified?
16. What is the Simple Digital Cash Protocol?
17. What is the Blinded Signature? How is it made?
18. Electronic money: What is token money and how their validness can be checked? Examples?
19. Electronic money: Why Simple Digital Cash protocol does not provide anonymity to customer?
20. Electronic money: What does it mean – “blinded token”? Why is it called so? How blinding-un-blinding is made? Examples?
21. XML: What is XML encryption?
22. XML: What is XML signature?