**Problem Session CMSE-353 “Security of Software Systems” 18.11.2021**

**Security requirements, Access control models, RSA, Digital signatures, Certificates, MD5**

1. What CIA concepts are?
2. What Authenticity, Assurance, Anonymity are?
3. What are the classes of intruders? What insider is? External intruder?
4. How intrusion can be detected?
5. What are the types of malware?
6. What are the methods of password cracking?
7. What are the requirements to strong passwords?
8. What social engineering is? What are the methods of SE?
9. What is Access Control Matrix? List? Capability list?
10. What is Mandatory Access Model? What rules are used in it?
11. What RSA method is? How many keys RSA has? How RSA keys are defined? How a private RSA key is defined? Public? How in RSA a message is encrypted? Decrypted?
12. RSA: key generation, Euclid GCD algorithm, Extended Euclidean algorithm, finding multiplicative inverse, Euler totient function, encryption/decryption, exponentiation by squaring with in-line reducing

Keys shall be relatively prime to fi(N)=(p-1)(q-1)=fi(p)\*fi(q), fi is Euler totient function; N=p\*q

Gcd(a,b)=1=>a,b are relatively prime; gcd(a,0)=a

Gcd(103, 24)=gcd(24, 103 mod 24)=gcd(24, 7)=gcd(7, 24 mod 7)=gcd(7,3)=gcd(3,7 mod 3)=gcd(3,1)=gcd(1,0)=1

Gcd(a,b)=gcd(b, a mod b = a-q\*b, q=floor(a/b))

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}.

E\*d=1 mod fi(N)

Extended Euclidean algorithm (m,b) b^(-1) mod m

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



A=(A1,A2,A3)=(1,0,m); B=(B1,B2,B3)=(0,1,b)

Step 1: B3=0=> A3 is gcd(A3,B3)=gcd(m,b)<>1 => inverse does not exist

B3=1=>gcd(m,b)=1=>inverse exists and b^(-1) mod m= B2; B1=m^(-1) mod b

Iteration

Q=floor(A3/B3);

T=A-q\*B=(A1-q\*B1, A2-q\*B2, A3-q\*B3 = A3 mod B3)

A=B;

B=T;

Goto Step 1;

C=M^e mod N; M=C^d mod N

Exponentiation use squaring together with reduction

M^(2k) mod N= (M^k mod N)^2 mod N

29=16+8+4+1

M^29 mod N=M^(16+8+4+1) mod N=(M^16 mod N)\*(M^8 mod N)\*(M^4 mod N)\*M

M^2 mod N =M2<N

M^4 mod N = M2^2 mod N =M4

M^8 mod N=M4^2 mod N =M8

M^16 mod N = M8^2 mod N =M16

M^29 mod N=) (M16\*M8 mod N)\*M4 mod N)\*M mod N

1. Can RSA be used for secret data transmission? How it can be done?
2. What digital signature is? How RSA digital signature can be constructed? What hash function is? Why hashing is used in RSA signature?
3. What certificate is? What for certificates are issued? Who issues certificates? What is the main information in a certificate? How a certificate is verified?
4. MD5: Message padding: target size, structure of the last block, padding bits structure, padding bits number
5. MD5: Initialization of the registers A, B, C, D
6. MD5: General structure using HMD5
7. MD5: Structure of HMD5
8. MD5: Round function of HMD5 structure
9. MD5: Logical functions, array T, array X, permutations $ρ\_{i}, i=2..4$, used in HMD5
10. MD5: What register is updated in one round function of HMD5?
11. MD5: How all for registers, A, B,C, D are updated in HMD5?
12. MD5: How many steps are used in a round function of HMD5?
13. MD5: What is the formula for a register updating in a round function of HMD5? How values of $k, i, s$ are defined for a particular step of a round function?