ECRYPT Problems preparing for the TEST #2

Problem # 1

Describe the ElGamal signature algorithm and prove that verification formula is true when the signature parameters are correct

Signature generation

a : random integer $(1 \leq a \leq p)$
p: large random prime
k: generator of Z_p^*

Entity A should do the following

a) select a random integer k, $1 \leq k \leq p-2$ with $gcd(k, p-1)=1$
b) compute $r=\alpha^k (mod\, p)$
c) compute $k^{-1} mod(p-1)$
d) compute $s=k-1(k(m)-ar) mod(p-1)$
e) A's signature for m is the pair (r,s)

Verification

$y=\alpha^a mod\, p$

To verify A's signature (r,s) on m, B should do the following
a) Obtain A's authentic public key (p,α,y)
b) Verify that $1 \leq r \leq p-1$; if not, reject the signature
c) Compute $V_1=y^r r^s$ mod p
d) Compute h(m) and $V_2=\alpha^{h(m)} mod\, p$
e)accept the signature if and oly if $V_1=V_2$

Problem # 2

Describe the Nyberg-Rueppel signature algorithm and prove that verification formula is true when the signature parameters are correct.

Same parameters from before

Signature generation

Entity A should :
a) compute ñ=R(m)
b) select a random integer k, 1<=k<=q-1, and compute r=a^-k mod p
c) compute e=ñ r mod p
d) compute s = a e + k mod q
e) A's signature for m is the pair (e,s)

Signature verification

To verify A's signature (e,s) on m, B should do the following

a) obtais A's authentic public key (p,q, α ,y)

b) Verify that 0<e<p if not, reject the signature
c) Verify that 0 <= s <= q; if not, reject the signature
d) compute $v=\alpha^{s}y^{-e} mod\, p$ and $\tilde{n}=v\,e\,mod\,p$
e) verify that $\tilde{n}\in M_R$ if $\tilde{n}\notin M_R$ then reject the sign
f) recover $m=R^{-1}(\tilde{n})$

Problem # 3
Solve the following set of congruencies :

$$x\equiv 6\,(mod\,7)$$
$$x\equiv 4\,(mod\,5)$$
$$x\equiv 10\,(mod\,11)$$
$$x\equiv 12\,(mod\,13)$$
$$x\equiv 16\,(mod\,17)$$

x = 5·11·13·17 + 7·11·13·17 + 7·5·13·17 + 7·5·11·17 + 7·5·11·13 =
mod 7 mod 5 mod 11 mod 13 mod 17

= 12155 + 17017 + 7735 + 6545 + 5005
mod 7 mod 5 mod 11 mod 13 mod 17

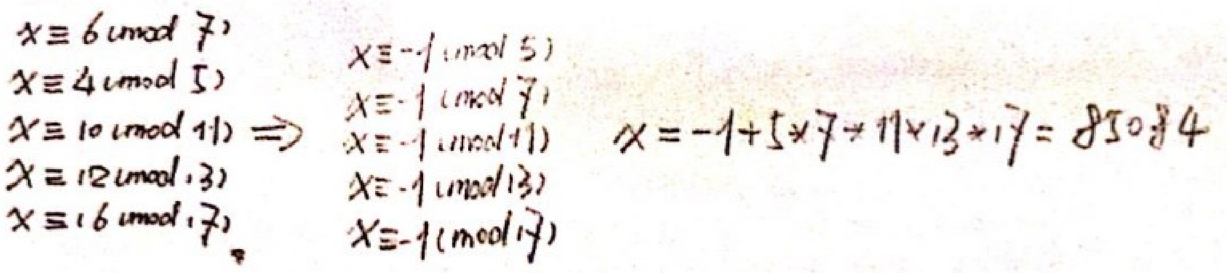
Before continuing looking for x, we need to verify we can apply the chinise remainder theorem:
gcd(7,5), gcd(7,11)=1, gcd(7,17)=1 (all are primes so the result is always 1)

mod 7:
x=12155(mod 7) → x=3 (mod 7) → we need a 6 instead of a 3
3 · 9 = 27 = 6(mod 7) → 12155 · 9

mod 5:
x=17017(mod 5) → x=2(mod 5) → we need a 4 instead of a 2
2·7 = 17 = 4(mod 5) → 17015·7

mod 11
x=7735(mod 11) -> 2(mod 11) = x → we need 10
2·6·10 = 1·20=10(mod 11)=7735·6·10

mod 13
x=6545(mod 10) → 6 (mod 13) → we need 12



$x\equiv 6\,(mod\,7)$
$x\equiv 4\,(mod\,5)$
$x\equiv 10\,(mod\,11)$ $\Rightarrow$
$x\equiv 12\,(mod\,13)$
$x\equiv 16\,(mod\,17)$

$x\equiv -1\,(mod\,5)$
$x\equiv -1\,(mod\,7)$
$x\equiv -1\,(mod\,11)$
$x\equiv -1\,(mod\,13)$
$x\equiv -1\,(mod\,17)$

$x=-1+5\times 7\times 11\times 13\times 17=85084$

Problem # 4
Assume we use RSA (with $n=p\cdot n$) and we have two cryptograms c_1 and c_2 of the same plain text message m which are ciphered with two different public keys e_1 and e_2 , GCD(e_1,e_2) . Prove that we can in easy way compute the plain text message (without private keys).

Theorem:
If a,b in Z then there are x, y in Z such as:
xa + yb = gcd(a,b)
by definition of the RSA system: $c_1 \equiv m^{e_1}(mod\, n)$; $c_2 = m^{e_2}(mod\, n)$
so: $c_1^a = (m^{e_1})^a (mod\, n)$ $c_2 \equiv (m^{e_2})^b (mod\, n)$

we can write

$$c_1^a * c_1^b = (m^{e_1})^a * (m^{c_2})$$
$$c_1^a * c_2^b = m^{(e_1 \cdot a + e_2 \cdot b)} * (mod\, n)$$

with the theorem
if $a,b,c,d \in Z$ and $n \in W$ $,n \geq 2$ and a $a \equiv b(mod\, n)$, $c \equiv d(mod\, n)$
then $a+c \equiv b+d(mod\, n)$ and $a \cdot c \equiv b \cdot d(mod\, n)$

with the beginning we can write

$$c_1^a * c_2^b \equiv m(mod\, n)$$

we then need to calculate a and b, we can do that using the euler extended algotithm

Problem # 5
Find the last 4 decimal digits of the number 2^{10^6} using Chinese Remainder Theorem.

<u>Theorem</u> (chinise remainder)

If m_1,m_2,…, m_r in N , gcd ($m_{i,}m_j$)= 1 for every i<>j;
Then for every a_1, a_2,…,a_r in Z a set of congurencies:

$$X \equiv a_1(mod\, m_1)$$
$$X \equiv a_2(mod\, m_2)$$
$$\vdots$$
$$X \equiv a_r(mod\, m_r)$$

Has exactly one solution x_0 in a set <o, m-1> (M= $m_{1,}$ m_2, ...m_r) and there are constants $c_{1,}c_{2,},...c_r$ and all solutions of the set of congruencies are given by the formula.

X_k=X_o +k * M; k in Z

Problem # 6
Assume we have two independent random variables X_1 , X_2 with values in the set $Z_2 = \{0,1\}$.
Prove that if X_2 has a uniform distribution then $X_1 \oplus X_2$ has also the uniform distribution. (This fact is known from the protocol “coin tossing by phone”)

1.At first we prove that the function $Y = X_1 \oplus X_2$ is a random variable. In general if (Ω, M) is a measurable space and $(E_t, \mathsf{F}_t)_{t\in T}$ is an arbitrary family of measurable spaces and for every $t \in T$ the function $f_t : \Omega \to E_t$ $(\mathsf{M}, \mathsf{F}_t)$ is measurable then the function $\underset{t\in T}{P} f_t : \Omega \to \underset{t\in T}{P} E_t$ is $(\mathsf{M}, \underset{t\in T}{P} \mathsf{F}_t)$ measurable too. Applying this general fact to our situation we have that the function (X_1, X_2) is $(\mathsf{M}, 2^{\{0,1\}} \otimes 2^{\{0,1\}})$ measurable. The function $S : \{0,1\} \times \{0,1\} \ni (x_1, x_2) \to x_1 \oplus x_2 \in \{0,1\}$ is of course $(2^{\{0,1\}} \otimes 2^{\{0,1\}}, 2^{\{0,1\}})$ measurable then $Y = X_1 \oplus X_2$ as a superposition of two measurable functions (X_1, X_2) and S is $(\mathsf{M}, 2^{\{0,1\}})$ measurable then it is a random variable.

2. Now we prove that the probability distribution of the random variable $Y = X_1 \oplus X_2$ is uniform. Denote

$$A_1 = \{\omega \in \Omega; X_1(\omega) = 1, X_2(\omega) = 0\}, \qquad B_1 = \{\omega \in \Omega; X_1(\omega) = 0, X_2(\omega) = 1\}$$
$$A_0 = \{\omega \in \Omega; X_1(\omega) = 0, X_2(\omega) = 0\}, \qquad B_0 = \{\omega \in \Omega; X_1(\omega) = 1, X_2(\omega) = 1\}$$

Sets A_0, A_1, B_0, B_1 are disjoint in pairs. Denote additionally $P(X_1 = 0) = p_0$, $P(X_1 = 1) = p_1$.
Random variables X_1 and X_2 are independent then we have

$$P(Y=1) = P(A_1 \cup B_1) = P(A_1) + P(B_1) = P(X_1 = 1) \cdot P(X_2 = 0) + P(X_1 = 0) \cdot P(X_2 = 1) = p_1 \cdot \frac{1}{2} + p_2 \cdot \frac{1}{2} = \frac{1}{2}$$

(because $p_0 + p_1 = 1$) and similarly

$$P(Y=0) = P(A_0 \cup B_0) = P(A_0) + P(B_0) = P(X_1 = 0) \cdot P(X_2 = 0) + P(X_1 = 1) \cdot P(X_2 = 1) = p_1 \cdot \frac{1}{2} + p_2 \cdot \frac{1}{2} = \frac{1}{2}$$

then the random variable $Y = X_1 \oplus X_2$ has the uniform probability distribution. ■

Problem # 7
Assume we have two independent random variables X₁ , X₂ with values in the set $Z_n = \{0,1,2\ldots,n-1\}$. Prove that if X₂ has a uniform distribution then $X_1 \oplus_n X_2$ has also the uniform distribution.

Problem # 8
Compute the following values: a) $\varphi(\varphi(5358))$, b) $\varphi(\varphi(3458))$, c) $\varphi(\varphi(2^{1000}))$, where φ is the Euler's function.

a)
$\varphi(\varphi(5358)) \to \varphi(2 \cdot 3 \cdot 19 \cdot 47) = 1 \cdot 2 \cdot 18 \cdot 46 = 1636 \to \varphi(1656) = \varphi(2^3 \cdot 3^2 \cdot 23) = (1 \cdot 2^2 \cdot 2 \cdot 31 \cdot 22) = 528$

b)
$\varphi(\varphi(3458)) \to \varphi(19 \cdot 13 \cdot 7 \cdot 2) \to 1 \cdot 6 \cdot 12 \cdot 18 = 1296 \to \varphi(1296) = \varphi(3^4 \cdot 2^4) = 2 \cdot 3^3 \cdot 1^3 = 432$

c)
$\varphi(\varphi(2^{1000})) = \varphi(2^{999}) = 2^{998}$

Problem # 9

Assume $GF(2^k)[x]$ (where k is a fixed natural number) is a ring of polynomials with coefficients in the field $GF(2^k)$. Prove that for every polynomial x^n (where $n\in N$) from $GF(2^k)[x]$ we have $x^n(mod(x^4+1))=x^{n(mod\,4)}$

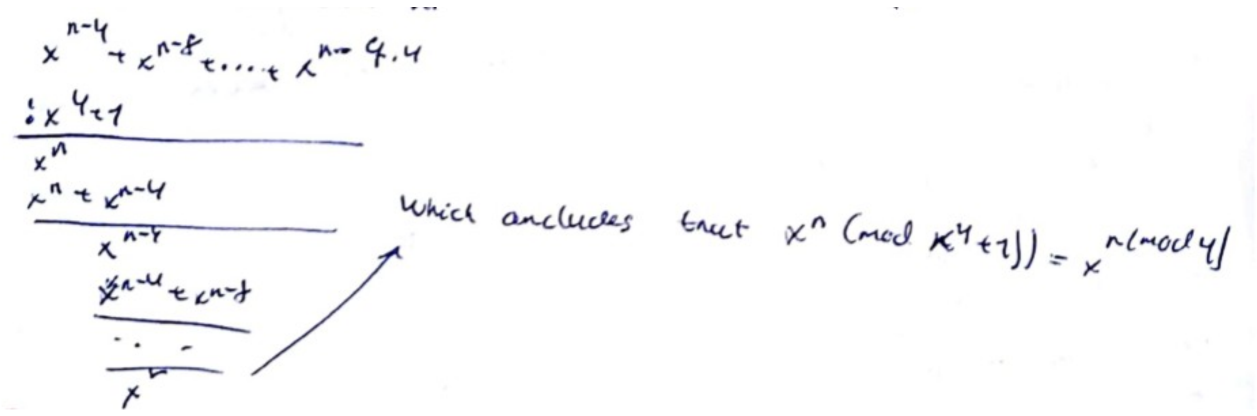
In Z_2={0,1} 1 oplus 1 = 0 and 0 oplus 0=0, so -a=a for a in Z_2 and a – 2b=a oplus b where a – 2 is a modulo 2 subtraction

$a=a_1,a_2,\dots,a_k\in GF(2^k)$ where $a_i\in\{0,1\}$ and $b=b_1,b_2,\dots,b_k\in GF(2^k)$ where $bi\in\{0,1\}$

$a+b=\{a_1\oplus_2 b_1, a_2\oplus_2 b_2,\dots,a_k\oplus_2 b_k\}$ e and the same is for a – 2 b

for n<4 equation is always true and for n>=4 there exists suh q in N that n=q·4+r (0<r<4) where r equiv n (mod 4)

Also we observe dividing polynomial (x^n for n>=4, stating that Z_2 addition and subtraction are identical)



$x^{n-4} + x^{n-8} + \dots + x^{n-q\cdot 4}$

$: x^4+1$

x^n

$x^n + x^{n-4}$

x^{n-4}

$\cancel{x}^{n-4} + x^{n-8}$

$\dots$

x^r

Which ancludes that $x^n (mod\ x^4+1)) = x^{n(mod 4)}$

Problem # 10

How many times we have to repeat experiments in the cave of Zero Knowledge to obtain probability of fraud less then 100^{-10} .

Nor For a probability of fraud of 2^{-t}, the protocol is iterated + times. $2^{-t} = 10^{10}$ <=> $\log_2(2^{-t}) = \log^2(10^{-10})$ <=> $-t = \log_2(10^{-10})$ => $t = -\log_2(10^{-10})$ → $t=-\log_2(10^{-10})$ t= + 33,22

2^{-kt} → we can suppose k=1 so we only change t

Problem # 11

Describe the Fiat-Shamir entity authentication protocol. How many times we have to repeat the Fiat-Shamir protocol to obtain the probability of error less than 100^{-100} .

1) One time setup

a) A trusted center t selects and published an RSA-like modalus but keeps primes p and q secret.

b) Each claimant A selects a secret s coprime to n, 1 < s <n-1, computes $v=s^2$ mod n, and registers V with T as itspublic key

$100^{-100}=2^{-t}$ <=> $\log_2(2^{-t}) = -t = \log_2(100^{-100})$ → $t=-\log_2(100^{-100})$

2) protocol messages:
each of t rounds has three messages with form as

A → B : $x=r^2 \, mod\, n(1)$
A ← B : $e\in\{0,\}(2)$
A → B : $y=r\cdot s^e(3)$

3)
For the Fiat-Shamir identification protocol, we have the following actions.
The Following steps are iterated t times

a) A chooses a random r (1<r<r-1) and sends x= r^2 (mod n) to B n= pq, p primes and que secret
b) B randomly selects a bit e=0 or e=1, and sends C to A
c) A computes and sends to B y, either y=r (if e=0) or y= rs (mod n), (if e=1).
d) B rejects the proof if y=0, and otherwise accepts upon verifying $y^2\equiv x\cdot v^e(mod\, n)$
(Depending on e, y^2=x or y^2=xv (mod n), since v= s^2 (mod n).
Note that checking for y=0 precludes the curse r=0)

Problem # 12
Assume we test primality of odd natural numbers with the probabilistic Miller-Rabin test. Assess probability of the fact that an odd composite number n is accepted as a prime for a given security parameter $t\in N$.

Can the Miller-Rabin test qualify a prime as a composite number ?

Miller-robin(n,t)
1) Write n-1=2^s r such that r is odd
2)
Input #1: *n* > 3, an odd integer to be tested for primality

```
Input #2: k, the number of rounds of testing to perform
Output: "composite" if n is found to be composite, "probably prime" otherwise

write n as $2^r\cdot d$ + 1 with d odd (by factoring out powers of 2 from n − 1)
WitnessLoop: repeat k times:
   pick a random integer a in the range [2, n − 2]
   x ← $a^d$ mod n
   if x = 1 or x = n − 1 then
      continue WitnessLoop
   repeat r − 1 times:
      x ← $x^2$ mod n
      if x = n − 1 then
         continue WitnessLoop
   return "composite"
return "probably prime"
```

How many experiments (random choices of the basis a) we have to do to be sure with probability $\geq 1-10^{-1000}$ that the tested number n is a prime

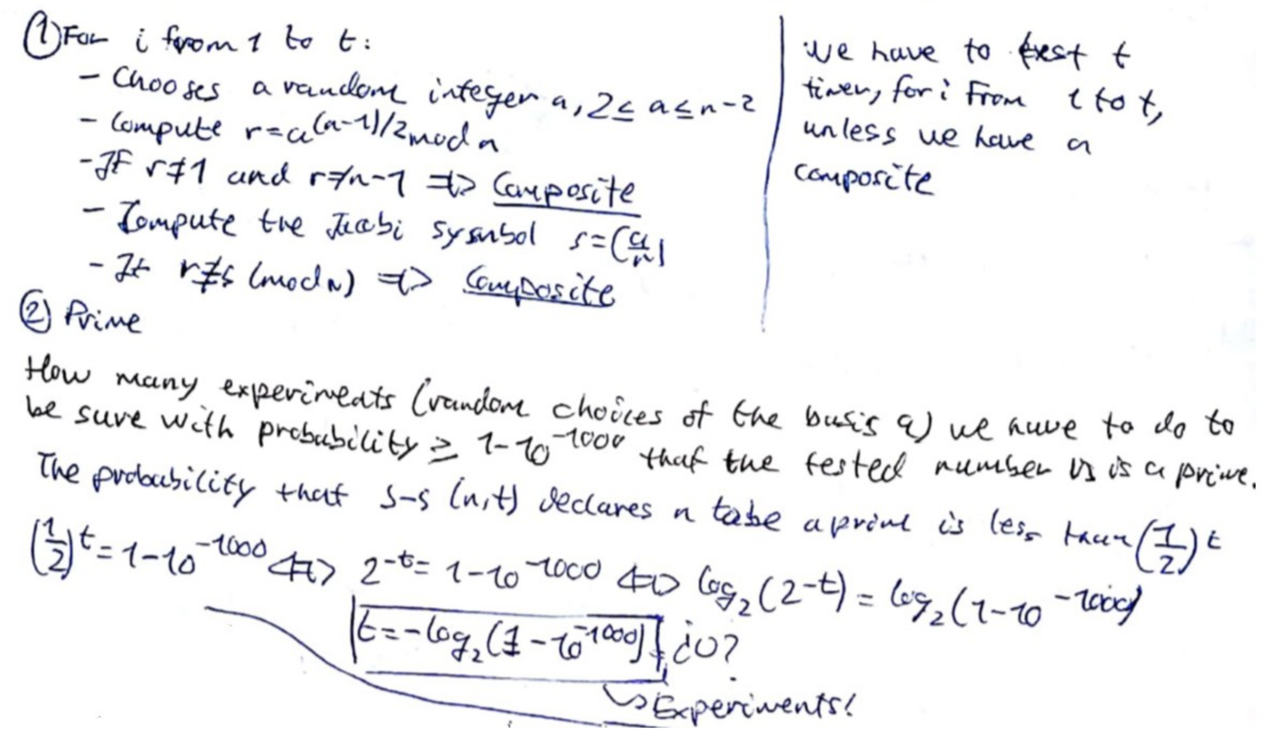
the probability that declares n to be prime is less than $(\frac{1}{4})^t$ → $(\frac{1}{4})^t=1-10^{-1000}$

Problem # 13

Assume we test primality of natural numbers with the probabilistic Solovay-Strassen test. Assess probability of the fact that an odd composite number n is accepted as a prime for a given security parameter $t \in N$.

Can the Solovay-Strassen test qualify a prime as a composite number ?

How many experiments (random choices of the basis a) we have to do to be sure with probability $\geq 1-10^{-1000}$ that the tested number n is a prime.



① For i from 1 to t:
- Chooses a random integer a, $2 \leq a \leq n-2$
- Compute $r = a^{(a-1)/2} \bmod n$
- If $r \neq 1$ and $r \neq n-1 \Rightarrow$ Composite
- Compute the Jacobi symbol $s = \left(\frac{a}{n}\right)$
- If $r \not\equiv s \pmod{n} \Rightarrow$ Composite

② Prime

We have to test t times, for i from 1 to t, unless we have a composite

How many experiments (random choices of the basis a) we have to do to be sure with probability $\geq 1-10^{-1000}$ that the tested number n is a prime.

The probability that S-S (n,t) declares n to be a prime is less than $\left(\frac{1}{2}\right)^t$

$\left(\frac{1}{2}\right)^t = 1-10^{-1000} \Leftrightarrow 2^{-t} = 1-10^{-1000} \Leftrightarrow \log_2(2^{-t}) = \log_2(1-10^{-1000})$

$\boxed{t = -\log_2(1-10^{-1000})}$ ¿O?

↳ Experiments!

Problem # 14

Describe the field F$_9$ (i.e, the field $GF(3^2)$).

A finite field contais a finite number of elements, the order is the number of elements

Existence and uniqueness of finite fuelds

1) if F is a finite field contains p^m elements for some prime p and integer $m \geq 1$, in our case, p=3 and m=2

2) For every prime power order 3^2, there is a unique (up to isomorphism) finite field of order p^m. this field is denoted by F$_2{}^3$=F$_9$, also GF (3^2)

* So F$_4$ is a finite field of orden 9, 3 a prime and characteristic of F$_9$. Also F$_9$ contains a copy of Z$_3$ as a subfield. Hence F$_9$ can be viewed as a extension field of Z$_3$ of degree 2

* The non-zero elements of F$_9$ form a group under multiplication called the multiplicative group F$^*_{9}$,which is a cyclic group of order 8

* Every subfield of F$_9$ has order 3^n, n a positive divison of 2

Problem # 15

What is it a pseudoprime number. Give an example of the pseudoprime number for the basis 2.

A pseudoprime is a probable prime that is not actually prime.
For any prime number p and any integer a such that p does not divide a (the pair are relatively prime) P divides exactly into $a^p - a$. Although a number n that does not divide exactly into a^n – a fro some a must be a composite number, the converse is not necessarily true.

For example a=2, n=341, a and n are relatively prime
and 341 divides exactly into 2^341 – 2
However 341=11*31, so it is a composite number
The smallest pseudoprime to basis 2 is 341

Problem # 16
Solve the following set of 4 congruencies

$x \equiv 3 (mod 5)$
$x \equiv 6 (mod 7)$
$x \equiv 7 (mod 11)$
$x \equiv 7 (mod 13)$

x= 7·11·13 + 5·11·13 + 5·7·13 + 5·7·11 =
mod 5 mod 7 mod 11 mod 13
= 1001 + 715 + 544 + 385

Before continuing with the problem we should check that we can apply the chinise remainder theorem

gcd(5,7)=1 gcd (5,11)= 1 … for all the same, the numbers are prime

mod 5
$x = 1001 \rightarrow x = 1 (mod 5)$ we need 3 instead of 1
$1 \cdot 8 = 3 (mod 5)$
1001·8

mod 7
$x = 715 \rightarrow x = 1 (mod 7)$ we need 6
$1 \cdot 13 = 6 (mod 7)$
715·13

mod 11
$x = 455 \rightarrow x = 4 (mod 11)$ we need 7 instead of 4
$4 \cdot 3 = 12 = 1 (mod 11)$
$4 \cdot 3 \cdot 18 = 216 = 7 (mod 11)$
455·3·18

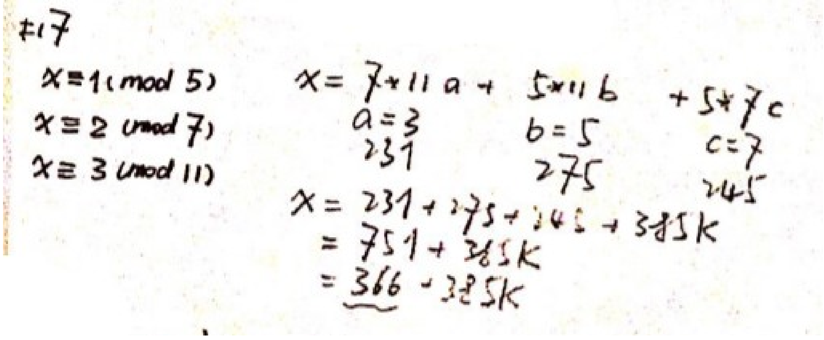
mod 13
$x = 385 \rightarrow x = 8 (mod 13)$ we need 7
$8 \cdot 5 = 40 = 1 (mod 13)$
$8 \cdot 5 \cdot 20 = 800 = 7 (mod 13)$
385·5·20
x=1001·8+715·13+455·3·18+385·5·20=80373
5·7·11·13=5005

$x \equiv 8037 (mod 5005) \rightarrow x \equiv 293 (mod\, 5005)$

Problem # 17

Solve the following set of 3 congruencies :

$x \equiv 1 (mod\, 5)$
$x \equiv 2 (mod\, 7)$
$x \equiv 3 (mod\, 11)$



#17

$x \equiv 1 (mod\ 5)$ $\quad x = 7*11\, a + 5*11\, b + 5*7\, c$

$x \equiv 2 (mod\ 7)$ $\quad a=3 \quad b=5 \quad c=7$

$x \equiv 3 (mod\ 11)$ $\quad 231 \quad 275 \quad 245$

$x = 231 + 275 + 245 + 385k$

$= 751 + 385k$

$= \underbrace{366}_{} - 385k$

Problem # 18

Assume we have a well defined RSA cryptosystem with $n = p \cdot q$, a public key e and a private key d . Is it possible that for some plain text messages m we have $m^6 (mod\, m) = m$? It would mean that there are messages $m \in Z_n$ which are not encrypted correctly.

$\Phi = (p-1)(q-1)$

Since that $ed \equiv 1 (mod\, \Phi)$, there exists an integer k such that $ed = I\, k\, \Phi$. Now, if gcd (m,p)=1 thereby Fermat's theorem:

$m^{p-1} = 1 (mod\, p)$

$m^{I\, k (p-1)(q-1)} \equiv m (mod\ p)$

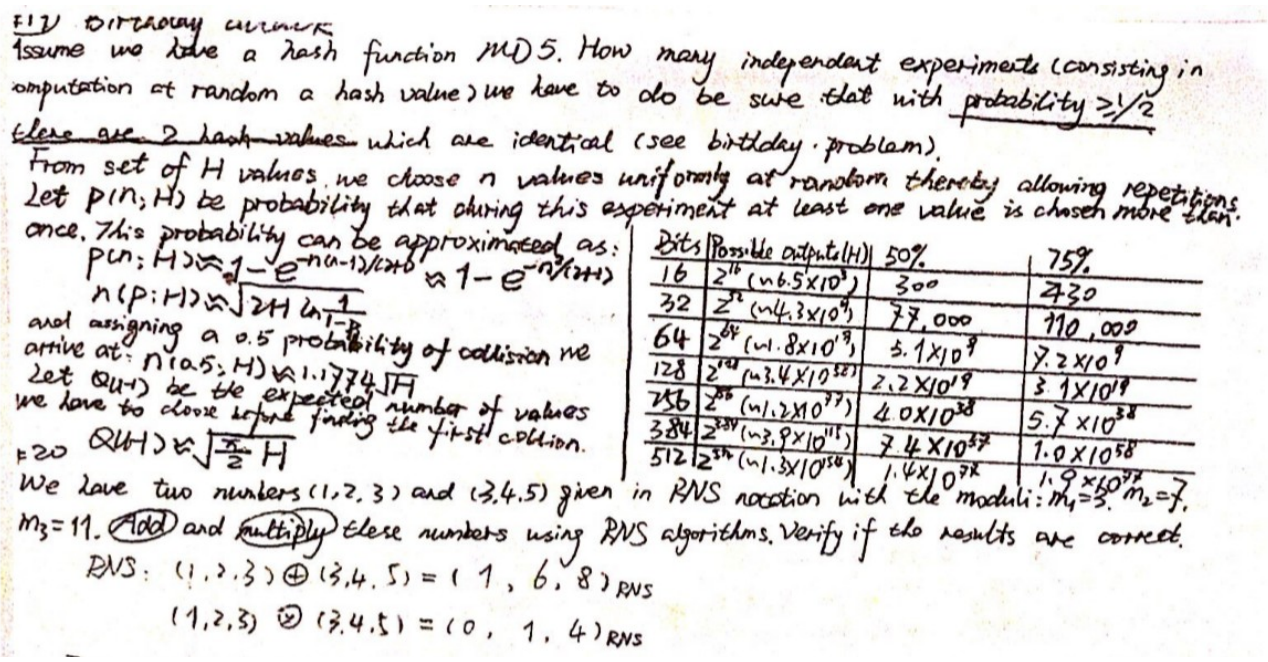
On the other hand, if gcd (m,p)=p, then this last congruence is again valid since each side is congruent to 0 mod p. hence in all cases:

$m^{ed} \equiv m (mod\ p)$ Also $m^{ed} \equiv m (mod\, q)$ As n and q are distinct primes: $m^{ed} \equiv m (mod\, n)$

Now for our example first d should be d=1, so we hare m^e=$m^{ed,}$ then, n should be n=m, which it’s difficult but possible as n depends on random primer p and q. So for this wind of message and d=1 it’s possible

Problem # 19

Assume we have a hash function MD5. How many independent experiments (consisting in computation at random a hash value) we have to do to be sure that with probability $\geq 1/2$ there are 2 hash values which are identical (see birthday problem).



#19 Birthday attack

Assume we have a hash function MD5. How many independent experiments (consisting in computation at random a hash value) we have to do be sure that with probability ≥1/2 there are 2 hash values which are identical (see birthday problem).

From set of H values we choose n values uniformly at random thereby allowing repetitions. Let p(n; H) be probability that during this experiment at least one value is chosen more than once. This probability can be approximated as:

$p(n;H) \approx 1-e^{-n(n-1)/(2H)} \approx 1-e^{-n^2/(2H)}$

$n(p;H) \approx \sqrt{2H \ln\frac{1}{1-p}}$

and assigning a 0.5 probability of collision we arrive at: $n(0.5;H) \approx 1.1774\sqrt{H}$

Let Q(H) be the expected number of values we have to choose before finding the first collision.

$Q(H) \approx \sqrt{\frac{\pi}{2}H}$

Bits	Possible outputs (H)	50%	75%
16	2^{16} ($\sim 6.5\times10^3$)	300	430
32	2^{32} ($\sim 4.3\times10^9$)	77,000	110,000
64	2^{64} ($\sim 1.8\times10^{19}$)	5.1×10^9	7.2×10^9
128	2^{128} ($\sim 3.4\times10^{38}$)	2.2×10^{19}	3.1×10^{19}
256	2^{256} ($\sim 1.2\times10^{77}$)	4.0×10^{38}	5.7×10^{38}
384	2^{384} ($\sim 3.9\times10^{115}$)	7.4×10^{57}	1.0×10^{58}
512	2^{512} ($\sim 1.3\times10^{154}$)	1.4×10^{77}	1.9×10^{77}

#20 We have two numbers (1,2,3) and (3,4,5) given in RNS notation with the moduli: $m_1=3$, $m_2=7$, $m_3=11$. Add and multiply these numbers using RNS algorithms. Verify if the results are correct.

RNS: $(1,2,3) \oplus (3,4,5) = (1, 6, 8)_{RNS}$

$(1,2,3) \otimes (3,4,5) = (0, 1, 4)_{RNS}$

Problem # 20

We have two numbers (1,2,3) and (3,4,5) given in RNS notation with the moduli: $m_1=3$, $m_1=7$, $m_3=11$. Add and multiply these numbers using RNS algorithms. Verify if the results are correct.

Definition

IF $v(x)=(v_1, v_2, \dots, v_t)$ and $v(y)=(u1,u2,\dots u_r)$

* $v(x)+ v/y))=(w1,w2,\dots,w_t)$

$w_i=v_1+w_i \pmod{m_i}$

* $v(x).v/y)=(z_1,z_2,\dots,z_t)$

where $z_i=v_{i.}.w_i \pmod{m_i}$

Resolution

→(1,2,3)+(3,4,5)= (4(mod 3), 6(mod 7), 8(mod 11)=(1,6,8)

→(1,2,3)+(3,4,5)= (3 (mod 3), 8(mod 7), 15(mod 11)=(0,1,4)

$M=m_1 \cdot m_2 \cdot m_3=3\cdot7\cdot11=231$

Problem # 21

Define the Diffie-Hellman protocol of key exchanging. Why is it a secure protocol ?

Diffie-Hellmar Key agreement: A and B each send the other one message over an open channel

1: One time setup An appropriate prime p and generator α of $Z_p^*\left(2\le\alpha\le p^{-2}\right)$ are selected and published.

2: Protocol messages

A→ B: α^x mod p (1)

A← B: α^y mod p (2)

3: Protocol actions Perform the following steps each time a shared key is required

a) A chooses a random secret x, 1<=x <=p^{-2}, and sends B message (1).
b) B chooses a random secret y, 1<=y <=p^{-2}, and sends A message (2).
c) B receives α^x and computes the shared key as $K=(\alpha^x)^y$ mod. P
d) A receives α^y and computes the shared key as $K=(\alpha^y)^x$ mod p

<u>Secure protocol</u>

Allowing two parties, never having met in advance or shared keying material, to establish a shared secret by exchanging messages over an open channel. The security rest on the intractability of the diffie-hellman theorem

Problem # 22

Compute values of the following Legendre's symbols

a) $\left(\frac{35}{7}\right)$

b) $\left(\frac{64}{5}\right)$

a) $\left(\frac{35}{7}\right)=\left(\frac{35(mod\,7)}{7}\right)=\left(\frac{0}{7}\right)=0$

b) $\left(\frac{64}{5}\right)=\left(\frac{64(mod\,5)}{5}\right)=\left(\frac{4}{5}\right)=\left(\frac{2}{5}\right)\cdot\left(\frac{2}{5}\right)=1$

Problem # 23

Compute values of the following Legendre's symbols knowing that 1097 is a prime.

a) $\left(\frac{5}{1097}\right)$

b) $\left(\frac{7}{1097}\right)$

c) $\left(\frac{2}{1097}\right)$

a)
From the law of quadratic reciprocity we have

$$\left(\frac{5}{1097}\right)\cdot\left(\frac{1097}{5}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{1097-1}{2}}=1$$

but $\left(\frac{1097}{5}\right)=\left(\frac{1097(mod5)}{5}\right)=\left(\frac{2}{5}\right)=-1$ the also $\left(\frac{5}{1097}\right)=-1$

b)

$$\left(\frac{7}{1097}\right)\cdot\left(\frac{1097}{7}\right)=(-1)^{\frac{7-1}{2}\cdot\frac{1097-1}{2}}=(-1)^{1644}=1$$

but $\left(\frac{1097}{7}\right)=\left(\frac{1097(mod\,7)}{7}\right)=\left(\frac{5}{7}\right)=-1$ the also $\left(\frac{7}{1097}\right)=-1$

c)

From a general property of the Legendre symbol we have for every odd prime p

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$

then $\left(\frac{2}{1097}\right)=(-1)^{(p^2-1)/8}$