Lisa Maszkiewicz

1	2	3	4	5	6

Problem Set #5 4/19/20

2. i) $N > 0 \in \mathbb{Z}$, $x | 20$, $x \neq 1, 2, 5$

Factors of $N = 1, 2, 4, 5, 10, 20$

Possible values of $\boxed{x = 4, 10, 20}$ $\boxed{\text{i.e. } x=4,\ x=10, \text{ or } x=20}$

ii) Let p, q be primes s.t. $p = 2q+1$. Let $\alpha \in \mathbb{Z}_p^*$.

Prove: If neither $\alpha^2 \pmod p$ nor $\alpha^q \pmod p = 1$, then α is a generator of $\mathbb{Z}_p^*$.

~~Def: A generator of $\mathbb{Z}_p^*$ is an element of $\mathbb{Z}_p^*$ with order $\phi(p)$.~~ We can also use Thm 7.5 that the order of any $a \in \mathbb{Z}_p^*$ divides $\phi(p)$.

Because p is prime, by Thm 4.2 ii)

$\phi(p) = p-1$ $\quad p = 2q+1$ Combining these 2 factors: $\phi(p) = p-1 = \boxed{2q = \phi(p)}$. So the ~~order of~~ generator has an order ~~$\phi(p)$~~ which divides $\phi(p) = 2q$. By Euler's Thm (4.4), we know $a \perp m$ because $a \in \mathbb{Z}_p^*$ that $a^{\phi(m)} \equiv 1 \bmod p$.

By def. order is the first value k, for which $a^k \equiv 1 \bmod p$. So if the order ~~is~~ only has factors 2 and q. ($2 | 2q$ and $q | 2q$), then as long as $a^2 \not\equiv 1 \bmod p$ and $a^q \not\equiv 1 \bmod p$, then $a^{\phi(m)} \equiv 1 \bmod p$ and a is a generator!

Lisa Maszkiewicz

Problem Set #5

4. i) El Gamal Decryption: To recover m:

Compute $y = \gamma^{p-1-a} \bmod p$

Compute $y \cdot \delta \bmod p = m$

First thing to notice is that y will not change

$\gamma = g^k \bmod p$ if γ, p, and a don't change. So,

$y \cdot \delta_1 \bmod p = m_1$; solve for y:

$y = m_1 \cdot \delta^{-1} \bmod p$. We can substitute this into an equation for m_2.

$m_2 = y \cdot \delta_2 \bmod p \Rightarrow \boxed{m_2 = (m_1 \cdot \delta^{-1} \bmod p) \cdot \delta_2 \bmod p}$

This is why γ ($\gamma = g^k \bmod p$), aka k needs to change each message!

ii) m1 derived in PDF portion. (m2 = 1,809)

5. i) If we start by subtracting : $s_1 - s_2 =$

$= k^{-1}(h(m_1) - ar) \bmod (p-1) - k^{-1}(h(m_2) - ar) \bmod (p-1)$

$= k^{-1}[h(m_1) - h(m_2) \cancel{-ar} \cancel{+ar}] \bmod (p-1)$

$s_1 - s_2 = k^{-1}(h(m_1) - h(m_2)) \bmod (p-1)$

By Thm 5.2 we can use the fact that $\gcd(s_1 - s_2, p-1) = 1$ and know $s_1 - s_2$ has a multiplicative inverse:

$[(s_1 - s_2)^{-1} \bmod (p-1)][k^{-1} \bmod (p-1)][s_1 - s_2 = k^{-1}(h(m_1) - h(m_2)) \bmod (p-1)]$

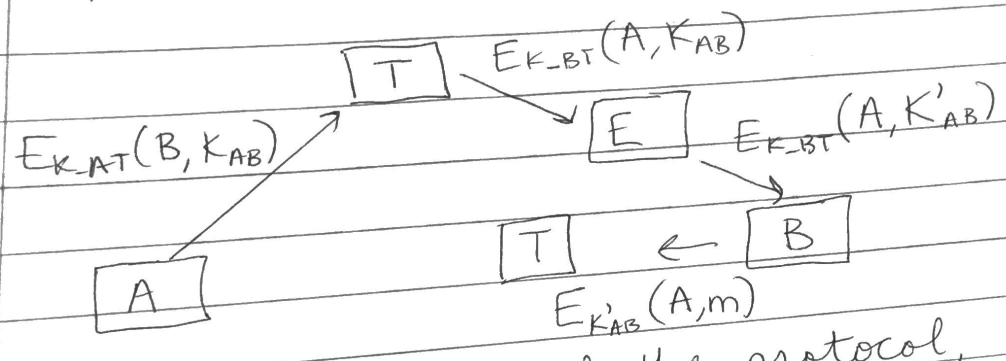
$\Rightarrow \boxed{k = (s_1 - s_2)^{-1}(h(m_1) - h(m_2)) \bmod (p-1)}$

ii) k was solved for in PDF

Lisa Maszkiewicz

Problem Set #5

6. In this case, I believe we can simply do a replay attack.



From previous runs of the protocol, Earl has recorded $E_{K\_BT}(A, K'_{AB})$. Earl has also discovered the value of the old session key K'_{AB}. Now he can just intercept~~s~~ Bob's attempted message to Alice.

3. Show that if h_1 is collision resistant, so is h_2. A.K.A. show that we can efficiently find a collision for h_1, given a collision for h_2.

Suppose $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$, $h_2 : \{0,1\}^{4m} \to \{0,1\}^m$ as follows

1. $x \in \{0,1\}^{4m}$ as $x = x_1 || x_2$, where $x_1, x_2 \in \{0,1\}^{2m}$
2. define $h_2(x) = h_1(h_1(x_1)||h_1(x_2))$

If there's a collision for h_2, then we have some $c, d \in \mathbb{Z}$ where $h_2(c) = h_2(d)$, so some $c = h_1(h_1(x_1)||h_1(x_2)) = d$

3. cont. because we already have a c and such that $c = d = h_1(h_1(x_1) \| h_1(x_2))$, it will be trivial to find 2 xs that can make up those h_1(values) combined. Especially because since we've already found h_2 we know the h_1s were used to find it.