Pham Hoang Long Do
NetID: 2995060

Homework 5

Problem 1

1. This is False since Bob will know that Eve is not the person that he supposes to talk with since he will verify what Eve sent to him using the k that Bob and Alice establised before. The security of the MAC still depend of the secretcy of the key. In addition, Alice and Bob use an increment counter. Therefore, any attempt to intervene or replaying the message will be detected.
2. This new protocol **is not secured**. Since Eve can use two previous messages (The second and the third message) to XOR them together. The part $y = PRG(k)$ will be cancelled out. That leaves Eve with the result:

$$2 \parallel A- > B \parallel N_A \parallel N_B \oplus 3 \parallel B < -A \parallel N_A \parallel N_B$$

   - This is unsecure since now Eve can basically have every information and can establish his own communication with Bob.
3. Yes. This protocol will remain secure. We basically establish **session counter** for each handshake we make. The security is still guaranteed as what we did in question 1.1.

Problem 2

1. Like what we discussed in class, we need a variable called δ which is tolerance delay. We need to do the following check on each side when they recieve the information:
   (a) Alice send Bob her T_A, and Bob also need to have Alice's previous T_A on his file. Lets call it T_A'. The first check is to compare if this is a new message by comparing $T_A > T_A'$.
   (b) The second check is when Bob records his own current time, called it T_B. He uses his T_B to subtract the tolerance delay δ to see if the message arrive on time or not. Then he compare the following $T_A > T_B - \delta$
   (c) Repeat the two above checks for new handshakes.
2. This will not impact the security. Since every PRP is a PRF, and every PRF is a MAC. Therefore, when we encrypt the full input, the output will still satistfies the condidion of a MAC. Hence, it will provide the same security as we were using a Mac.
3. **Yes** if the GSM protocol is compromised, then the attacker has the ability to initiate handshake with **different sessions** using the information that he spoofed on the **previous sessions**

Problem 3

1. $185 \cdot 11^{150} + 1230 \cdot 1024^{33} \mod 41$
   - Using property 1.2:

$$(185 \cdot 11^{150} \mod 41 + 1230 \cdot 1024^{33} \mod 41) \mod 41$$

   - Using property 1.4:

$$((185 \mod 41)(11^{150} \mod 41) + (1230 \mod 41)(1024^{33} \mod 41)) \mod 41$$

- Using property 1.5:

$$(21(11 \mod 41)^{150} + 0 \cdot (1024^{33} \mod 41)) \mod 41 = (21 \cdot (11)^{150}) \mod 41$$

- Since 41 is a prime number, we using 1.5 and 1.9 together:

$$\begin{aligned}((21 \mod 41) \cdot 11^{150 \mod \phi(41)} \mod 41) \mod 41 &= (21 \cdot 11^{150 \mod 40} \mod 41) \mod 41\\ &= 21 \cdot 11^{30} \mod 41\\ &= 672 \mod 41 = 16\end{aligned}$$

2. $645(19850^{874000} + 653 \cdot 123456^{9856}) \mod 29$
   - Using property 1.4:

$$((645 \mod 29) \cdot (19850^{874000} + 653 \cdot 123456^{9856}) \mod 29) \mod 29$$

- Using property 1.2:

$$7 \cdot ((((19850)^{874000} \mod 29) + (653 \cdot 123456^{9856} \mod 29)) \mod 29) \mod 29$$

- Using property 1.9, since 29 is a prime number:

$$(7 \cdot (19856^{874000 \mod 28} \mod 29) + ((653 \mod 29) \cdot (123456)^{9856 \mod 28} \mod 29) \mod 29) \mod 29$$

- Simplify:

$$\begin{aligned}(7 \cdot (14^8 + (15 \cdot (123456)^0 \mod 29)) \mod 29) \mod 29 &= (7 \cdot (14^8 + 15 \mod 29) \mod 29) \mod 29\\ &= (7 \cdot (1475789071) \mod 29) \mod 29\\ &= (7 * 9) \mod 29\\ &= 63 \mod 29\\ &= 5\end{aligned}$$

3. $\frac{513}{12} + \frac{704}{11} + 20450 \mod 103$
   - change to the inverse form:

$$513 \cdot 12^{-1} + 704 \cdot 12^{-1} + 20450 \mod 103$$

- Using property 1.2:

$$(513 \cdot 12^{-1} \mod 103 + 704 \cdot 11^{-1} \mod 103 + (20450 \mod 103)) \mod 103$$

- Using multiplicative inverse, we have $(12 * 43) \mod 103 = 1$. Therefore, $12^{-1} = 43$. Similarly, $(11 * 75) \mod 103 = 1$. Therefore, $11^{-1} = 75$:

$$\begin{aligned}(513 \cdot 43 \mod 103 + (704 \cdot 75) \mod 103 + 56) \mod 103 &= (17 + 64 + 56) \mod 103\\ &= 137 \mod 103\\ &= 34\end{aligned}$$

4. $248 - \frac{45}{123456} + \frac{1785}{32 \cdot 2} \mod 86$
- This is **not valid** since we can't find the multiplicative inverse of 123456 and $32 \cdot 2$ such that $123456 \cdot X \mod 86 = 1$ and $32 \cdot 2 \cdot Y \mod 86 = 1$ where X, Y are the multiplicative inverse.

5. $245 \cdot (17 + (421 \cdot 8^{109}(32^{590} + 7996))) \mod 59$

- Using property 1.4:

$$(245 \mod 59 \cdot (17 + (421 \cdot 8^{109}(32^{590} + 7996))) \mod 59) \mod 59$$

- Using property 1.2:

$$(245 \mod 59 \cdot (17 \mod 59 + (421 \cdot 8^{109} \cdot (32^{590} + 7996) \mod 59) \mod 59) \mod 59) \mod 59$$

- Using property 1.4:

$$(245 \mod 59 \cdot (17 \mod 59 + (421 \mod 59 \cdot 8^{109}(32^{590} + 7996)) \mod 59) \mod 59) \mod 59$$

- Using property 1.4:

$$(245 \mod 59 \cdot (17 \mod 59 + (421 \mod 59 \cdot (8^{109} \mod 59(32^{590} \mod 59 + 7996 \mod 59) \mod 59) \mod 59) \mod 59) \mod 59$$

- Using property 1.2:

$$(245 \mod 59 \cdot (17 \mod 59 + (421 \mod 59 \cdot (32^{590} \mod 59 + 7996 \mod 59) \mod 59) \mod 59) \mod 59) \mod 59$$

- Using Lemma 1.4:

$$(245 \mod 59 \cdot (17 \mod 59 + (421 \mod 59 \cdot (8^{109 mod \phi(59)} \mod 59(32^{590 \mod \phi(59)} \mod 59) +7996 \mod 59) \mod 59) \mod 59) \mod 59) \mod 59) \mod 59$$

$$(245 \mod 59 \cdot (17 \mod 59 + (421 \mod 59 \cdot (8^{109 mod 58} \mod 59(32^{590 \mod 58} \mod 59) +7996 \mod 59) \mod 59) \mod 59) \mod 59) \mod 59) \mod 59$$

$$(245 \mod 59 \cdot (17 \mod 59 + (421 \mod 59 \cdot (8^{51} \mod 59(32^{10} \mod 59) +7996 \mod 59) \mod 59) \mod 59) \mod 59) \mod 59) \mod 59$$

- Using property 1.5:

$$\begin{aligned}
&(245 \mod 59 \cdot (17 \mod 59 + (421 \mod 59 \cdot ((8 \mod 59)^{51}((32 \mod 59)^{10} + 7996 \mod 59) \\
&\qquad \mod 59) \mod 59) \mod 59) \mod 59) \mod 59 \\
&= (9 \cdot 17 + (8 \cdot (8^{51}(32^{10} + 31) \mod 59) \mod 59) \mod 59) \mod 59 \\
&= (9 \cdot (17 + (8 \cdot (8^{51} \cdot 34) \mod 59) \mod 59) \mod 59) \mod 59 \\
&= (9 \cdot (17 + (8 \cdot 28) \mod 59) \mod 59) \mod 59 \\
&= (9 \cdot (17 + 47) \mod 59) \mod 59 \\
&= 45 \mod 59 \\
&= 45.
\end{aligned}$$

6. $\phi(43)+\phi(1680)$ (First represent each of 43 and 1680 as a product of powers of distinct primes and then compute the Euler's function.)

$$\begin{aligned}43 &= 43^1 \\ 1680 &= 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^1 \\ \phi(43) &= (43^1 - 43^0) = 42 \\ \phi(1680) &= (2^4 - 2^3)(3^1 - 3^0)(5^1 - 5^0)(7^1 - 7^0) = 384\end{aligned}$$

- Hence:

$$\phi(43) + \phi(1680) = 42 + 384 = 426$$

7. Is the following congruence true? why?
$13 \cdot 4 \equiv 93 \cdot 6 \pmod{19}$
- They are not congruence since:

$$\begin{aligned}\text{Left Side} &= 13 \cdot 4 \mod 19 \\ \text{Using 1.4} &= ((13 \mod 19) \cdot (4 \mod 19)) \mod 19 \\ &= (13 \cdot 4) \mod 19 \\ &= 52 \mod 19 = 14\end{aligned}$$

$$\begin{aligned}\text{Right Side} &= 93 \cdot 6 \mod 19 \\ \text{Using 1.4} &= ((93 \mod 19) \cdot (6 \mod 19)) \mod 19 \\ &= (17 \cdot 6) \mod 19 \\ &= 102 \mod 19 = 7\end{aligned}$$

- Since Right Side $\neq$ Left Side. Therefore, it is **not congruent**.