Solutions to Homework Assignment # 10

1. (a) $6292^b \equiv x \bmod n \Rightarrow$ valid signature
   (b) $4768^b \neq x \bmod n \Rightarrow$ invalid signature
   (c) $1424^b \equiv x \bmod n \Rightarrow$ valid signature

2. (a) $sig_{K_{pr}}(x) = x^a \bmod n = y$
   $ver_{K_{pub}}(x,y): \qquad x \stackrel{?}{\equiv} y^b \bmod n$
   Assume that a has l bits.
   Using the square & multiply algorithm, the average signing will take:
   $\# \otimes \approx l$ squarings $+ \frac{1}{2} \cdot l$ multiplications $= \underline{\frac{3}{2} \cdot l}$
   Since $b = 2^{16} + 1 \equiv 65537 \equiv 10000000000000001_2$, the average verification takes:
   $\# \otimes = 16\ squarings + 1\ multiplication = 17$

   (b) Signing takes longer than verification.

   (c)

l [bits]	T_{unit}	n	$\frac{T_{unit}}{operation}$	$T(sig)$	$T(ver)$
512	100 ns	16	25.6 μs	19.7 ms	435.2 μs
1024	100 ns	32	102.4 μs	157.3 ms	1.741 ms

   (d) $T(1\otimes) = (\frac{l}{8})^2 \cdot \frac{1}{f}$; time for one multiplication modulo p

$$T(sig) = \frac{3}{2} \cdot l \cdot \frac{T_{unit}}{operation} = 0.5\ s$$

$$\frac{T_{unit}}{operation} = \frac{l}{8}^2 \cdot T_{unit}$$

$$F \geq \frac{1}{T_{unit}} [Hz]$$

   i) $\underline{6.29\ MHz}$
   ii) $\underline{50.33\ MHz}$

3. birthday attack: $k \approx \sqrt{n \cdot m \cdot \frac{1}{1-\varepsilon}}$

n	$\varepsilon = 0.5$	$\varepsilon = 0.1$
2^{64}	$3.6 \cdot 10^9$	$1.4 \cdot 10^9$
2^{128}	$1.5 \cdot 10^{19}$	$6.0 \cdot 10^{18}$
2^{160}	$1.5 \cdot 10^{24}$	$3.9 \cdot 10^{23}$

   number of messages after which probability for collision is ε

4. Birthday paradox: Take random x_1 and compute $h(x_1)$. Store in table $(h(x_1), x_1)$. Compute $h((x_2), x_2)$ for a second (random) value x_2. Check whether $h(x_1) = h(x_2)$. If not, enter in table {item sorted by the $h(x_i)$ values}. Compute $h((x_3), x_3)$ for a third (random) value x_3. Check whether $h(x_3) = h(x_1)$ or $h(x_3) = h(x_2)$. If not, enter in table, again sorted by the $h(x_i)$ values. Continue until your current hash value $h(x_j)$ corresponding to the current x_j is already in the table as $h(x_i)$. Now x_j and x_i collide. The average memory requirement is $\mathcal{O}(2^{n/2})$ memory locations.