Číslo cvičení: 9
Jméno: Marek Bryša
UČO: 323771
Login: xbrysa1

1. (a) $4586^{107} = 1 \mod 7919$, q is prime.
   (b) $v = 4586^{-55} = 1175 \mod 7919$
   (c) $\gamma = 4586^{29} = 48 \mod 7919$
   (d) $y = 29 + 55 \cdot 61 = 3384 \mod 7919$
   (e) $4586^{3384} \cdot 1175^{61} = 48 = \gamma \mod 7919$

2. The father can use Shamir's $(5, 3)$-threshold scheme, where the eldest son receives 2 pieces of the secret and the others get 1 each.

3. (a) Not a MAC. Considering a chosen message attack we would authentize $(a||b, e_k(a||b))$ and $(c||d, e_k(c||d))$. Then we could forge $a||d$ and $c||b$. The same applies if a man-in-the-middle intercepts two different messages.
   (b) Not a MAC. Reason is the same as in (a).
   (c) Not a MAC. Intercepting a single message is sufficient to authentize any permutation of its m_i submessages.

4. $l_0 = \frac{x-3}{1-3} \cdot \frac{x-7}{1-7} = x^2/12 - (5x)/6 + 7/4$
   $l_1 = \frac{x-1}{3-1} \cdot \frac{x-7}{3-7} = -x^2/8 + x - 7/8$
   $l_2 = \frac{x-1}{7-1} \cdot \frac{x-3}{7-3} = x^2/24 - x/6 + 1/8$
   $f(x) = 28l_0 + 31l_1 + 17l_2 = -(5x^2)/6 + (29x)/6 + 24$
   $S = f(0) = 24$

5. (a) Bob accepts iff $y^e = RX_A^f \mod n$.
   (b) $Y = y^e = (rx_A^f)^e = RX_A^f \mod n$.
   (c) In step (i) Eve chooses $R = X_a^{f(e-1)}$. In step (iii) Eve sends $y = X_A^f$. Then $Y = X_A^{fe}$ and $RX_A^f = X_A^{f(e-1)} X_A^f = X_A^{fe} \implies$ Bob accepts.

6. For each group of $t - 1$ scientists there must be at least one unique lock that they cannot open. And if a new scientist join the group, he must be able to open it. Hence there must be at least $\binom{n}{t-1} = \binom{11}{5} = 462 = L$ locks.
   Each group of t scientists must be able to open the locks so at least $n - t + 1$ must posses the keys. Each must therefore have $\frac{n-t+1}{n} \cdot L = 252$ keys.