Exercises: Hashing and Digital Signatures

Exercises

1. For each of the following hash functions, find two message values m_1 and m_2 such that $\#(m_1) = \#(m_2)$:

   (a) Messages are simply plaintext phrases, e.g., 'This message is made of words.' The hash function is defined by $\#(m) =$ number of words in m. E.g., $\#$('The revolution will not be televised') $= 6$.

   (b) Messages are elements $m \in \mathbb{N}$. The hash function is defined by $\#(m) = m \mod 1024$.

   (c) Messages are elements $\{n \in \mathbb{N} \mid 0 \leq n \leq 255\}$. The hash function is defined by $\#(m)$ being the number of 1s in the binary representation of m. E.g., $\#(123) = \#(0111\,1011_2) = 6$.

   (d) Messages are elements $\{n \in \mathbb{N} \mid 0 \leq n \leq 255\}$. Let $L(m)$ be the left four bits of the 8-bit binary representation of m and let $R(m)$ be the right four bits of the 8-bit binary representation of m. The hash function is defined by $\#(m) = L(m) \oplus R(m)$. E.g., $\#(123) = 0111 \oplus 1011 = 1100$.

2. Alice has set up her public RSA key as $(n_A, e_A) = (1003, 65)$. Bob has set up his public RSA key as $(n_B, e_B) = (1007, 41)$. They both agree to sign their messages using the third hash function described above: $\#(m)$ is the number of 1s in the 8-bit binary representation of m.

   (a) Bob wants to send the message $m = 321$ to Alice. Encrypt m using Alice's public key by calculating $m^{e_A} \mod n_A$.

   (b) Calculate $\#(m)$.

   (c) Calculate Bob's private key d_B.

   (d) Sign $\#(m)$ by calculating $\#(m)^{d_B} \mod n_B$.

   (e) Calculate Alice's private key d_A.

   (f) Show that $(m^{e_A})^{d_A} = m \mod n_A$ and $(\#(m)^{d_B})^{e_B} = \#(m) \mod n_B$.

Answers

1. For each of the following hash functions, find two message values m_1 and m_2 such that $\#(m_1) = \#(m_2)$:

   (a) #('Mathematics') = #('Security')

   (b) For any message value m: $m = m+1024 \mod 1024$. So taking $m_1 = 1$, we can find $m_2 = 1 + 1024 = 1025$. Then $m_1 = 1 = 1025 = m_2 \mod 1024$.

   (c) Let $m_1 = 1$ and $m_2 = 2$. The binary representations of these values are 0000 0001 and 0000 0010, respectively. So $\#(1) = \#(2)$.

   (d) Let $m_1 = 18$ and $m_2 = 3$. The binary representations of these values are 0001 0010 and 0000 0011, respectively. Then $\#(m_1) = 0011 = \#(m_2)$.

2. Alice has set up her public RSA key as $(n_A, e_A) = (1003, 65)$. Bob has set up his public RSA key as $(n_B, e_B) = (1007, 41)$. They both agree to sign their messages using the third hash function described above: $\#(m)$ is the number of 1s in the 8-bit binary representation of m.

   (a) Bob wants to send the message $m = 321$ to Alice. Encrypt m using Alice's public key by calculating $m^{e_A} \mod n_A$.

   $$m^{e_A} = 321^{65} = 287 \mod 1003$$

   (b) Calculate $\#(m)$.

   $$\#(m) = \#(321) = \#(1\,0100\,0001_2) = 3$$

   (c) Calculate Bob's private key d_B.

   $$d_B = 137$$

   (d) Sign $\#(m)$ by calculating $\#(m)^{d_B} \mod n_B$.

   $$\#(m)^{d_B} = 3^{137} = 675 \mod 1007$$

   (e) Calculate Alice's private key d_A.

   $$d_A = 257$$

   (f) Show that $(m^{e_A})^{d_A} = m \mod n_A$ and $(\#(m)^{d_B})^{e_B} = \#(m) \mod n_B$.

   $$(m^{e_A})^{d_A} = 287^{257} = 321 \mod 1007$$

   $$(\#(m)^{d_B})^{e_B} = 675^{41} = 3 \mod 1003$$

Practicing RSA

Try the following randomisable question. Make sure that you can perform the calculations by hand and use your spreadsheets to check your answers. **Test**

Yourself Visit the URL below to try a numbas exam:
`https://numbas.mathcentre.ac.uk/question/155037/rsa-encryption/embed/`