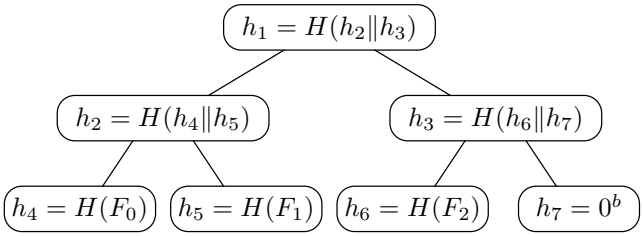
11 Security II (MGK)

(*a*) An RSA encryption routine calculates the value $m^e \bmod n$ using a square-and-multiply algorithm. During the execution of that algorithm, you can briefly hear a buzzing sound (through radio-frequency interference) on an AM radio receiver located near the computer. You record that sound, and discover that it is actually the following sequence of two different sounds A and B: $BABAABABAAB$. What is the value of e? [6 marks]

(*b*) MHash implements a hash function over file sequences $F_0, F_1, \ldots, F_{n-1} \in \{0,1\}^*$ with $n > 0$, using a collision-resistant hash function $H : \{0,1\}^* \to \{0,1\}^b$:

MHash$(n, F_0, F_1, \ldots, F_{n-1})$:
  $d := \lceil \log_2 n \rceil$
  for $i := 0$ **to** $n - 1$
    $h_{2^d+i} := H(F_i)$
  for $i := n$ **to** $2^d - 1$
    $h_{2^d+i} := 0^b$
  for $i := 2^d - 1$ **downto** 1
    $h_i := H(h_{2i} \| h_{2i+1})$
  return h_1

Example calculation for $n = 3$:



(*i*) Show that MHash is not collision resistant if n is not fixed, by constructing two different sequences of files that result in the same output h_1. [8 marks]

(*ii*) Suggest an improvement to MHash to make it collision resistant. [6 marks]