5 Cryptography (mgk25)

(*a*) (*i*) One way to use a secure hash function H to form a message-authentication code is the construct $\mathsf{Mac}_K(M) = H(K\|M)$. What problem with that approach does the HMAC construct solve? [4 marks]

(*ii*) Why does the HMAC construct pad the key? [2 marks]

(*b*) Your opponent has started using *HomeBrew*, a new block cipher $C = E_K(M)$ that they invented last week. It uses a 96-bit key $K = K_1\|\ldots\|K_{12}$, where each of the 12 bytes K_i ($1 \leq i \leq 12$) is used as an 8-bit subkey in one of the 12 rounds that apply a keyed permutation f:

$R_0 := M$
for $i := 1$ **to** 12
  $R_i := f_{K_i}(R_{i-1})$
$C := R_{12}$

Describe an attack to find K for this type of block cipher that is practical for an adversary with a computer fast enough to execute such a block cipher around 2^{50} times and that can store and lookup around 2^{50} keys and messages. [6 marks]

(*c*) Your colleague has proposed the following digital signature algorithm. Let $(\mathbb{G}, q, g)$ be system-wide choices of a cyclic group $\mathbb{G}$ of prime order q with generator g such that the discrete logarithm problem in $\mathbb{G}$ is computationally infeasible. Further let $H : \{0,1\}^* \to \mathbb{Z}_q^*$ be a collision-resistant hash function. Pick a secret key $x \in \mathbb{Z}_q$ uniformly at random and let (y, r) with $y := g^x \in \mathbb{G}$ and $r := H(g^{H(x)})$ be the corresponding public key.

Then use as the signature of message $m \in \{0,1\}^*$ the value $s \in \mathbb{Z}_q^*$ found by solving

$$H(x) \cdot s \equiv x \cdot r + H(m) \pmod q$$

for $s = [H(x)]^{-1} \cdot [x \cdot r + H(m)]$. (Here a^{-1} denotes the multiplicative inverse of finite-field element $a \in \mathbb{Z}_q^*$. Your colleague considers $\mathbb{P}(s = 0)$ negligible.)

The recipient, given $(\mathbb{G}, q, g, H), (y, r), (m, s)$ verifies that signature by checking the equation

$$H\left(y^{r \cdot s^{-1}} g^{H(m) \cdot s^{-1}}\right) = r$$

Show that this signature scheme does not provide existential unforgability. [8 marks]