Problem Set 6

Alex Miller

December 2, 2021

Abstract

Collaborators: Elizabeth Coble, Lucy Li

1 1

I wrote some code to test my solution; I'll paste it below:

```python
# Our psudeocode
def double_mod_exp(a, b, c, d, N):
    ac = (a * c) % N

    b_bits = BitArray(uint=b, length=b.bit_length())
    d_bits = BitArray(uint=d, length=d.bit_length())

    res = 1
    for b_bit, d_bit in zip(b_bits, d_bits):
        res = (res ** 2) % N
        if b_bit and d_bit:
            res = (res * ac) % N
        elif b_bit:
            res = (res * a) % N
        elif d_bit:
            res = (res * c) % N
    return res
```

My algorithm, in the worst case (where $b = c = 2^n - 1$), makes $2n + 1$ calls to MUL and $2n + 1$ calls to MOD.

It is correct because in all cases it multiples res by the correct combination of a and c according to each's respective exponent.

2 2

2.1 a

The best case runtime occurs when $2^{n-1} \geq b = 2^{n-1} < 2^n$. In this case, $b_2 = 1||0^{n-1}$ and only one bit of b is set to 1. Therefore $MOD - EXP$ only makes $n + 1$ calls to MUL and $n + 1$ calls to MOD.

2.2 b

The worst case runtime occurs when $2^{n-1} \geq b = 2^n - 1 < 2^n$. In this case, $b_2 = 1^n$ and all the bits of b are set to 1. Therefore $MOD - EXP$ makes $n + n = 2n$ calls to MUL and $n + n = 2n$ calls to MOD.

3 3

3.1 c

$\mathbb{G}$ is a group

1. $\exists e \in \mathbb{G} s.t. \forall g \in \mathbb{G}, e \circ g = g \circ e = g$

   The identity permutation $e : \Sigma \to \Sigma s.t. \forall x \in \Sigma, e(x) = x$ is in $\mathbb{G}$, since $e(A) = A$.

Moreover $\forall x \in \Sigma, \forall g \in \mathbb{G}, g(e(x)) = g(x) = e(g(x))$

Therefore $\forall g \in \mathbb{G}, g \circ e = g = e \circ g$

Therefore e is an identity for all $g \in \mathbb{G}$

QED

2. $\forall g \in \mathbb{G}, \exists h \in \mathbb{G} s.t. g \circ h = h \circ g = e$

   $\forall g \in \mathbb{G}$, with inverse g^{-1}, since $g(A) = A$, $g^{-1}(A) = A$. Therefore $\forall g \in \mathbb{G}$, $g^{-1} \in \mathbb{G}$

   Therefore, $\forall g \in \mathbb{G}, \exists h = g^{-1} \in \mathbb{G} s.t. \forall x \in \Sigma, g(h(x)) = h(g(x)) = e(x)$ (the identity permutation on Σ)

   Therefore $\forall g \in \mathbb{G}, \exists h \in \mathbb{G} s.t. g \circ h = h \circ g = e$

   QED

3. $\forall g_1, g_2, g_3 \in \mathbb{G}, (g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$. By simplification:

   $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

   $\forall x \in \Sigma, g_1(g_2(x)) \circ g_3 = g_1 \circ g_2(g_3(x))$

   $\forall x \in \Sigma, g_1(g_2(g_3(x))) = g_1(g_2(g_3(x)))$

   QED

3.2 d

$\mathbb{G}$ is **not** a group

1. $\exists e \in \mathbb{G} s.t. \forall g \in \mathbb{G}, e \circ g = g \circ e = g$

   The identity permutation $e : \Sigma \to \Sigma s.t. \forall x \in \Sigma, e(x) = x$ is in $\mathbb{G}$. (Given)

   Moreover $\forall x \in \Sigma, \forall g \in \mathbb{G}, g(e(x)) = g(x) = e(g(x))$

   Therefore $\forall g \in \mathbb{G}, g \circ e = g = e \circ g$

   Therefore e is an identity for all $g \in \mathbb{G}$

2. but, $\nexists g \in \mathbb{G}, \exists h \in \mathbb{G} s.t. g \circ h = h \circ g = e$

   Consider two permutations $\sigma, \delta \in \mathbb{G}$ s.t. $\sigma \neq e, \delta \neq e, \sigma \circ \delta = \delta \circ \sigma = e$ (σ and δ are inverses of one another)

   This implies that $\forall x \in \Sigma, \sigma(\delta(x)) = \delta(\sigma(x)) = e(x) = x$

   Therefore, for $x = A$, $\sigma(\delta(A)) = \delta(\sigma(A)) = e$

   Since for all $g \in \mathbb{G}, g \neq e, g(A) = B$, $\sigma(B) = \delta(B) = e(A) = A$

   Observe that for both σ and δ, $\sigma(B) = \delta(B) = A$.

   Therefore, for an member of $g \in \mathbb{G}, g \neq e$ to be invertible, $g(B) = A$

   Since this is not a quality of all members of $\mathbb{G}$, not all members of $\mathbb{G}$ are invertible

   QED

4 5

Consider any $m_0, m_1, c \in \mathbb{G}$, and some uniform random variable $\mathbf{k}$ on $\mathbb{G}$. Since m_0, m_1, c are constants, we can say that:

1. $Pr[\mathbf{k} = c \circ m_0^{-1}] = Pr[\mathbf{k} = c \circ m_1^{-1}] = \frac{1}{|\mathbb{G}|}$
2. $Pr[\mathbf{k} \circ m_0 = c \circ m_0^{-1} \circ m_0] = Pr[\mathbf{k} \circ m_1 = c \circ m_1^{-1} \circ m_1] = \frac{1}{|\mathbb{G}|}$ (Groups cancel)
3. $Pr[\mathbf{k} \circ m_0 = c \circ e] = Pr[\mathbf{k} \circ m_1 = c \circ e] = \frac{1}{|\mathbb{G}|}$ (def of Inverse)
4. $Pr[\mathbf{k} \circ m_0 = c] = Pr[\mathbf{k} \circ m_1 = c] = \frac{1}{|\mathbb{G}|}$ (def of Identity)
5. $Pr[E(\mathbf{k}, m_0) = c] = Pr[E(\mathbf{k}, m_1) = c] = \frac{1}{|\mathbb{G}|}$ (def of E)

Therefore E meets our definition of perfect secrecy.

5 6

Proof Steps:

1. First we combine all the elements in our group, and set it equivalent to itself:

   $g_1 \circ g_2 \circ ... \circ g_m = g_1 \circ g_2 \circ ... \circ g_m$ (valid)

2. Because our group is abelian we reorder one side of our equation to put inverses next to each other:

   $g_1 \circ g_2 \circ ... \circ g_m = g_7 \circ g_m \circ ... \circ g_2$ (NOT valid)

   Members of our group, besides our identity, can be inverses of themselves, in which case there is no way to place such members adjacent to their inverses. Reordering therefore does not cause the equation to cancel to the identity e.

6 9

The size of $|\mathbb{Z}_N^*|$, for $N = pq$, $= pq - p - q + 1$. Therefore the probability of uniformly randomly picking an element $\in \{0, 1, ..., N-1\}$ that is not in $\mathbb{Z}_N^*$ is:

$1 - Pr[\text{picking an element in } \mathbb{Z}_N^*] = 1 - \frac{pq-p-q+1}{pq} = \frac{pq-(pq-p-q+1)}{pq} = \frac{p+q-1}{pq} \approx \frac{p+q}{pq} = \frac{p}{pq} + \frac{q}{pq} = \frac{1}{q} + \frac{1}{p}$

Therefore when p and q are large (1024 bits long) the probability of choosing a value not in $\mathbb{Z}_N^*$ is $\approx \frac{1}{2^{1024}-1} + \frac{1}{2^{1024}-1} \approx 2 * \frac{1}{2^{1024}} \approx 2^{-1023}$