

Instructions

- Answer each question completely; justify your answers.
- This assignment is due at: 3:00 pm on Tuesday February 27th.

1. By \mathbb{Z}_n^* we denote the set $\{a \in \mathbb{Z}_n \mid \text{GCD}(a, n) = 1\}$. A *quadratic residue* modulo n is any element x of \mathbb{Z}_n^* that is a square (i.e., $x = y^2$ for some $y \in \mathbb{Z}_n^*$). What are the quadratic residues for

- (a) \mathbb{Z}_{23}^*
- (b) \mathbb{Z}_{26}^*
- (c) \mathbb{Z}_{27}^*

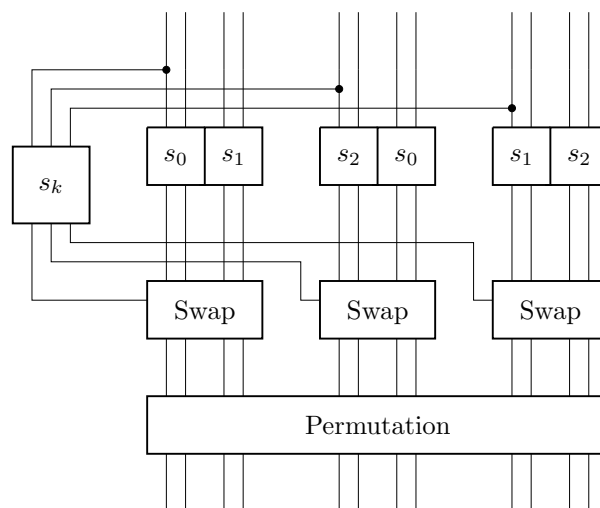
In a few weeks we will see in class how to determine whether a given element $x \in \mathbb{Z}_p^*$ is a quadratic residue, where p is a prime. For instance, we'll learn how to answer the question: Is 789 a quadratic residue in \mathbb{Z}_{5683}^* ?

2. Below is a schematic diagram for the function $f : \{0, 1\}^{12} \rightarrow \{0, 1\}^{12}$, which is used in each round of computation of an NDS-like cryptosystem in which $n = 12$ and $r = 16$.

The specifications of this cryptosystem are such that s_0 is the identity function, s_1 is the complement function, s_2 swaps the first and second bits, and the permutation in the final step of f simply reverses the order of the 12 bits.

You have gained access to an implementation of the encryption algorithm for this cryptosystem, using the key s_k that Alice and Bob have as their secret. This implementation is online on the course website.

- (a) How many possible choices are there for the key s_k ?
- (b) Perform a chosen plaintext attack on the cryptosystem, and thereby determine s_k .



A *group* (\mathcal{G}, \cdot) consists of a set \mathcal{G} along with a binary operation \cdot , such that:

- \mathcal{G} is closed under \cdot
- \cdot is associative (i.e., $a \cdot (b \cdot c) = (a \cdot b) \cdot c$)
- there exists an identity with respect to \cdot
(i.e., there exists an element $e \in \mathcal{G}$ such that $a \cdot e = e \cdot a = a$ for all $a \in \mathcal{G}$)
- each element has an inverse
(i.e., for each $a \in \mathcal{G}$ there exists an element $b \in \mathcal{G}$ such that $a \cdot b = b \cdot a = e$)

Note that we often refer to the group as \mathcal{G} rather than (\mathcal{G}, \cdot) . Notice also that \cdot need not be commutative; a group in which \cdot is commutative is called an *Abelian* group.

The notation a^n will be used to denote $\underbrace{a \cdot a \cdot a \cdots a}_{n \text{ a's}}$. The *order* of an element $a \in \mathcal{G}$ is the smallest positive integer t such that $a^t = e$. If a has order $|\mathcal{G}|$ then a is a *generator* of \mathcal{G} .

3. Find all generators of each of the following groups:

- (a) \mathbb{Z}_9^*
- (b) \mathbb{Z}_{15}^*
- (c) \mathbb{Z}_{17}^*
- (d) \mathbb{Z}_{25}^*

4. Prove the following statement:

If the order of $a \in \mathbb{Z}_n^*$ is t and $a^s \equiv 1 \pmod{n}$, then t divides s .

5. (a) Suppose that α is a generator of \mathbb{Z}_n^* . Prove that α^k is also a generator of \mathbb{Z}_n^* if and only if $\text{GCD}(k, \phi(n)) = 1$, where ϕ is Euler's totient function.
- (b) Provided that \mathbb{Z}_n^* has at least one generator, then how many generators does it have?
- (c) When p is prime, \mathbb{Z}_p^* is known to have a generator. How many generators are there in:
 - i. \mathbb{Z}_{19}^*
 - ii. \mathbb{Z}_{31}^*
 - iii. \mathbb{Z}_{181}^*
 - iv. \mathbb{Z}_{257}^*
 - v. $\mathbb{Z}_{2^t+1}^*$, where $(2^t + 1)$ is prime
 - vi. \mathbb{Z}_{2t+1}^* , where t and $(2t + 1)$ are prime

6. Algorithm 4.9 on page 162 of the Handbook of Applied Cryptography, is as follows:

Input: A multiplicative finite group \mathcal{G} of order n , an element $a \in \mathcal{G}$, and the prime factorisation $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

Output: The order t of a .

- 1 Set $t \leftarrow n$.
- 2 For $i = 1, 2, \dots, k$ do each of the following:
 - 2.1 Set $t \leftarrow \frac{t}{p_i^{e_i}}$.

2.2 Compute $b \leftarrow a^t$.

2.3 While b is not the multiplicative identity do the following: compute $b \leftarrow b^{p_i}$
and set $t \leftarrow tp_i$.

3 Return t .

Use this algorithm to determine the order of each of the following elements:

- (a) 5 in \mathbb{Z}_7^*
- (b) 12 in \mathbb{Z}_{25}^*
- (c) 3 in \mathbb{Z}_{61}^*

Which of these elements are generators?

7. Solve for x (i.e., find the smallest non-negative integer solution):

- (a) $5^x \equiv 4 \pmod{37}$
- (b) $6^x \equiv 16 \pmod{41}$
- (c) $13^x \equiv 12 \pmod{197}$
- (d) $55^x \equiv 444 \pmod{569}$

And for some additional chores for while I'm away:

- Read the paper “It is easy to determine whether a given integer is prime” by Andrew Granville, published in the Bulletin of the American Mathematical Society.
- Read about the Cryptographic Challenges sponsored by RSA.
- Read about the Elliptic Curve Cryptosystem (ECC) Challenge sponsored by Certicom.

Links pertinent to each of the above items are on the course website.