

M360 Mathematics of Information Security

exercise sheet # 6

Exercise # 1 (2 points)

Prove: $\{k \cdot m \mid k \in \mathbb{Z}\}$ is a subgroup of \mathbb{Z}_n if and only if m divides n .

Exercise # 2 (2 points)

Compute as many subgroups as possible of U_9 . Try to indicate their relationship w.r.t. set theoretic inclusion in form of a diagram. Bonus: Can you do the same for the affine group over \mathbb{Z}_3 ?

Exercise # 3 (2 points)

Let X be a set and S_X be the set of all maps from X to X which are one-to-one and onto. Verify that S_X is a group with respect to composition of mappings. If the order of X is finite, what is the order of the group S_X ? Bonus: If the order of X is finite, can you find a very large subgroup of S_X which is not equal to S_X ? If you wish, try an example for $|X| = 3$ or 4 .

Exercise # 4 (2 points)

Bob's public key is $(a, n) = (6679, 34189)$. You have intercepted a message from Alice to Bob. The RSA ciphertext is 33417. What is the plaintext? Hint: in case you want to use the Extended Euclidean Algorithm, an implementation is available from the course web page.

Exercise # 5 (2 points)

Why does every row and every column of the group table of a finite group show every element of the group exactly once? Show that the following table cannot be the table of a group.

	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>f</i>	<i>g</i>	<i>h</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>f</i>	<i>g</i>	<i>h</i>
<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>e</i>	<i>f</i>	<i>d</i>	<i>h</i>	<i>g</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>e</i>	<i>a</i>	<i>g</i>	<i>h</i>	<i>d</i>	<i>f</i>
<i>c</i>	<i>c</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>h</i>	<i>g</i>	<i>f</i>	<i>d</i>
<i>d</i>	<i>d</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>b</i>	<i>c</i>	<i>e</i>	<i>a</i>
<i>f</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>d</i>	<i>c</i>	<i>b</i>	<i>a</i>	<i>e</i>
<i>g</i>	<i>g</i>	<i>h</i>	<i>d</i>	<i>f</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>h</i>	<i>h</i>	<i>d</i>	<i>f</i>	<i>g</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>b</i>

due Friday, 10/21/05.