Cryptography
(Math 4613)
Challenge VI
Composing Cryptosystems

Paul L. Bailey

October 20, 2007

Definition 1. Let G be a group and let $X, Y \subset G$. Set

$$XY = \{xy \in G \mid x \in X \text{ and } y \in Y\} \quad \text{and} \quad X^{-1} = \{x^{-1} \in G \mid x \in X\}.$$

Definition 2. Let (A, K, E) and (A, K, F) be cryptosystem with the same alphabet and keyspace. The *composition* of these cryptosystems is the cryptosystem (A, K, Z) where

$$Z_k = E_k \circ F_k, \quad \text{for every } k \in K.$$

Problem 1. Let G be a group and let $H, K \leq G$. Show that $HK \leq G$ if and only if $HK = KH$.

Problem 2. Let G be a group, $H \leq G$, and $K \lhd G$. Show that $HK = KH$ and $HK \leq G$.

Problem 3. Let (A, K, E) and (A, K, F) be closed cryptosystems. Under what conditions is the composition (A, K, Z) closed?