INTRODUCTION

This manual presents the basic principles and techniques of cryptanalysts and their relation to cryptography. Cryptography concerns the various ways of protecting messages from being understood by anyone except those for whom the messages are intended. Cryptographers are the people who create and use codes and ciphers. Cryptanalytics is the art and science of solving unknown codes and ciphers. Cryptanalysts try to break the codes and ciphers created and used by cryptographers.

This publication is organized into six parts. Part One explains basic principles which apply to all the parts that follow. The following five parts each cover a major type of system and the cryptanalytic techniques that apply to it. Parts Two, Three, and Four each build on the techniques explained in the parts that precede them. A new student should study these in order. Parts Five and Six are largely independent of Parts Two through Four and can be used separately after Part One.

For practice in the techniques explained in this manual, the Army Correspondence Course Program offers a course in basic cryptanalysts. See the References Section at the back of this manual for further information.