The University of Sydney
Math3024 Elementary Cryptography and Protocols

Semester 1 **Exercises and Solutions for Week 2** 2004

Objectives. In this tutorial you should familiarize yourself with the `Magma` Computational Algebra System, learn to create and manipulate strings in `Magma` and to define and work with basic cryptographic constructs available in `Magma`.

1. *Magma overview:* Read over and work through the document "Introduction to Magma for Cryptography". You should become familiar with assignment (`:=`) in `Magma`, the concepts of parents and elements, with basic constructions of integers, rationals, strings in `Magma`, and with standard operators.

Solution Refer to the `Magma` tutorial for details of the language.

2. For each of the intrinsic functions

`RandomSubstitutionKey`, `StripEncoding`, and `SubstitutionEnciphering`,

type the function name followed by a semicolon at the prompt. The information displayed is called the signature of the function. What are the components of this information, and what does it tell you?

Solution The signature details the number and types of arguments an intrinsic function takes, and prints a short text description of its use. The intrinsic functions

`RandomSubstitutionKey`, `StripEncoding`, and `SubstitutionEnciphering`

are incorporated as member functions for substitution cryptosystems. You should be able to identify the versions which apply to cryptosystems and the versions which apply to strings.

3. Create the string in `Magma`

"I am standing up at the water's edge in my dream"

and assign it to the variable W. Next apply the function `StripEncoding` to W and reassign W to be the output. What is the encoded plaintext that you obtain?

Solution The strip encoding gives `IAMSTANDINGUPATTHEWATERSEDGEINMYDREAM`.

4. Define K to be the output of `RandomSubstitutionKey`. What is your key? Using K and W, use the function `SubstitutionEnciphering` to find the encipher W with respect to the key K. What is the ciphertext for W?

Solution The substitution key `UVLOIDTGKYZCRHBPMJQWXNFSAE` enciphers the above plaintext as `KURQWUHOKHTXPUWWGIFUWIJQIOTIKHRAOJIUR`.

5. Show that the deciphering map with respect to K is also a simple substitution. What is the inverse substitution key with respect to your particular K? Verify this by creating the inverse key and enciphering the ciphertext with respect to it.

Solution The inverse of the above substitution key is

YOLFZWHNERICQVDPSMXGABTUJK.