ASSIGNMENT 5 WRITEUP

Chris Moon

February 2023

1 Goal

My assignment 5 takeaways, and a short bit on cryptography.

2 TAKEAWAYS

GMP

-The Gnu Multi-precision library is helpful in handling arithmetic on large, decimal numbers, that C would typically struggle with.

-However, using mpz type variables requires setup and knowledge of the gmp library functions.

-Importantly, mpz types must be initialized before usage and cleared after.

-Also, the gmp functions usually don't return a value, instead directly changing the value of an "result" parameter passed to them.

SS encryption method, and cryptography

-The SS encryption method works via the creation of keys.

-the public key isn't hidden, and is used to encrypt data

-the private key is only seen by the creator, as is used to decrypt data encrypted by the public key

-SS encryption relies heavily on the multiplication of large prime numbers, since the products of prime numbers are harder to factor.

-file encryption is basically character by character

COMPILING MULTIPLE EXECUTABLES

-makefiles can compile multiple executables

-using make all: binary1, binary2, etc

IMPORTANCE OF CRYPTOGRAPHY, AND PERSONAL USES

-Cryptography and encryption is extremely useful when data is shared over the internet, especially when the data is often personal information, such as passwords, IDs, and contact information.

-Thus, encryption is used by some companies in their texting and email services. Google, for example, encrypts data on their gmail servers.

-Pushing to a remote repository requires the generation and sharing of keys for security, similar to how keys are generated for encryption