```
** Documentation

Below are two sample programs using OpenSSL's BIGNUM library.

You can find OpenSSL's documentation at the following URL by scrolling
down to the functions that begin "BN_". Not all functions are listed, so
sometimes you need to click on a related function and find it on that page.

https://www.openssl.org/docs/man1.1.1/man3/

The Google documentation is easier to find things and read, but is not 100%
compatible with the 1.1.1 documentation given above. Since testing will be on
a 1.1.1 system, do not use any function not listed in the above documentation.

https://commondatastorage.googleapis.com/chromium-boringssl-docs/bn.h.html

** Compiling

Be sure to #include <openssl/bn.h>

Read https://krovetz.net/152/openssl.html for information on compiling.

===== EXAMPLE 1: GCD


#include <openssl/bn.h>
#include <stdio.h>

void gcd(BIGNUM *r, BIGNUM *a, BIGNUM *b, BN_CTX *ctx)
{
    BIGNUM *c = BN_new();
    BIGNUM *d = BN_new();
    BIGNUM *td = BN_new();

    BN_copy(c,a);
    BN_copy(d,b);

    while ( ! BN_is_zero(d) ) {
        BN_copy(td,d);           // td = d
        BN_mod(d, c, td, ctx);   // d = c%td
        BN_copy(c,td);           // c=td
    }

    // Copy results
    BN_copy(r, c);               // r = c

    BN_free(c);
    BN_free(d);
    BN_free(td);
}


int main()
{
    unsigned char a[20] = {0xff};
    unsigned char b[20] = {0xee};

    BN_CTX *ctx = BN_CTX_new();

    BIGNUM *bna = BN_bin2bn(a, sizeof(a), NULL);
    BIGNUM *bnb = BN_bin2bn(b, sizeof(b), NULL);

    BIGNUM *r_me = BN_new();
    BIGNUM *r_ssl = BN_new();
```

```
    gcd(r_me, bna, bnb, ctx);
    BN_gcd(r_ssl, bna, bnb, ctx);

    if ( BN_cmp(r_ssl, r_me) != 0)
        printf("Not equal!\n");

    char *as = BN_bn2dec(bna);
    char *bs = BN_bn2dec(bnb);
    char *rs = BN_bn2dec(r_me);

    printf("GCD of\n%s\nand\n%s\nis\n%s\n",as,bs,rs);

    return 0;
}

/* Output:
GCD of
145579264656007907867945168883848503911040155648O
and
135873980345607380676748824291591936983637478604 8
is
97052843104005271911963445922565669274026770432
*/

===== EXAMPLE 2: I/O

#include <openssl/bn.h>
#include <stdio.h>

int main() {
    char a[100], b[100], c[100];
    scanf("%99s %99s %99s", a, b, c);

    BN_CTX *ctx = BN_CTX_new();
    BIGNUM *x = BN_new();
    BIGNUM *y = BN_new();
    BIGNUM *z = BN_new();
    BIGNUM *r = BN_new();
    BN_dec2bn(&x, a);       // BN_dec2bn wants BIGNUM ** instead of BIGNUM *
    BN_dec2bn(&y, b);
    BN_dec2bn(&z, c);

    BN_mul(x, x, y, ctx);
    BN_nnmod(r, x, z, ctx);

    char *res = BN_bn2dec(r);
    printf("%s\n", res);
    free(res);

    BN_CTX_free(ctx);
    BN_free(x);
    BN_free(y);
    BN_free(z);
    BN_free(r);
    return 0;
}
```