Universität des Saarlandes
Lehrstuhl für Softwaretechnik
Prof. Andreas Zeller, Stephan Neuhaus
Design of Secure Software Systems
Handout 3

1 Breaking *rand*(3) With TOD Seed

```c
#include <stdio.h>
#include <stdlib.h>

static const unsigned int sequence[] = {
   706062696, 388317246, 1795625833, 1641240349, 1013505830,
  1048427458, 1562911947,  836469238, 1567615431,   84389751,
};
int main() {
  unsigned int seed = 1069804800;
  int success = 0;
  int tries = -1;

  while (!success && tries < 10000000) {
    int i;

    tries++;
    srand(seed + tries);
    for (i = 0; i < sizeof(sequence)/sizeof(sequence[0]); i++) {
      if (rand() != sequence[i])
        break;
    }
    success = i == sizeof(sequence)/sizeof(sequence[0]);
  }
  if (success)
    printf("Seed is %u\n", seed + tries);
  else
    printf("No success\n");

  return 0;
}
```

2 Mixing with MD5

```c
#include <openssl/md5.h>

static void
digest_mix(unsigned char *digest, int random1, int random2) {
  MD5_CTX md5;
  unsigned char buf[sizeof(int)];
  int i;

  MD5_Init(&md5);
  for (i = 0; i < sizeof(int); i++) {
    buf[i] = random1 & 0xff;
    random1 = random1 >> 8;
  }
  MD5_Update(&md5, buf, sizeof(buf));
  for (i = 0; i < sizeof(int); i++) {
    buf[i] = random2 & 0xff;
    random2 = random2 >> 8;
  }
  MD5_Update(&md5, buf, sizeof(buf));
  MD5_Final(digest, &md5);
```

```
}
```

3 Extended Euclidean Algorithm

```
int egcd(int* a, int* b, int m, int n) {
  int a_prime = 1, b_prime = 0;
  int c = m, d = n;
  int q = c / d, r = c % d;

  *b = 1; *a = 0;

  /* am + bn = d; a_prime m + b_prime n = c = qd + r */
  while (r != 0) {
    int t;

    c = d; d = r;
    t = a_prime; a_prime = *a; *a = t - q*(*a);
    t = b_prime; b_prime = *b; *b = t - q*(*b);
    q = c / d; r = c % d;
    /* am + bn = d; a_prime m + b_prime n = c = qd + r */
  }

  /* am + bn = d = gcd(m, n) */
  return d;
}
```