# Midterm Review

ECE568 – Lecture 14

Courtney Gibson, P.Eng.
University of Toronto ECE

# Block vs. Stream Ciphers

List two advantages of block ciphers over stream ciphers.

# SSL / MACs

The SSL protocol uses a Message Authentication Code (MAC) to authenticate data being sent over SSL. List two advantages of using a MAC rather than a digital signature for authentication?

# Vulnerabilities

```
#define BUFLEN 128
01:void get_file(char *dst, char *src, char len) {
02:  int pos;
03:  char n;
04:
05:  for (n = 0; n < len; n++) {
06:    if (src[n] == '/') pos = n;
07:  }
08:  for (n = pos; n < len; n++) dst[n] = src[n];
09:}
10:int main(int argc, char **argv){
11:  int len;
12:  char buffer[BUFLEN];
13:  char file[BUFLEN+4];
14:
15:  /*strnlen(s, maxlen) returns the min of maxlen and strlen(s)*/
16:  len = strnlen(argv[1], BUFLEN);
17:  get_file(buffer, argv[1], len);
18:  sprintf(file, "%d%s", len, buffer);
19:  printf(file);
20:  return 0;
21:}
```

# Needham-Schroeder Protocol

1. **A → T :** $\{ A, B, N_A \}$
2. **T → A :** $\{ N_A, K_{AB}, B, \{K_{AB}, A\}_{KB} \}_{KA}$
3. **A → B :** $\{ K_{AB}, A \}_{KB}$
4. **B → A :** $\{ N_B \}_{KAB}$
5. **A → B :** $\{ (N_B - 1) \}_{KAB}$

- What attack is possible if "B" in step 2 was omitted from the protocol?
- What attack is possible if "$N_A$" in step 2 was omitted from the protocol?
- What attack is possible if "$(N_B - 1)$" in step 5 was omitted from the protocol?

# MACs and Signatures

Assume that Mallory is able to observe all messages sent between Alice and Bob. Mallory has no knowledge of any keys but the public keys used for digital signatures. State whether MAC and digital signatures protect against the four attacks described below. Given message X, the value of Auth(X) is computed using a MAC or a signature.

1) Alice sends a message X="Transfer $1000 to Mark" in the clear and Auth(X) to Bob. Mallory intercepts the message and replaces "Mark" with "Mallory". Will Bob detect it?

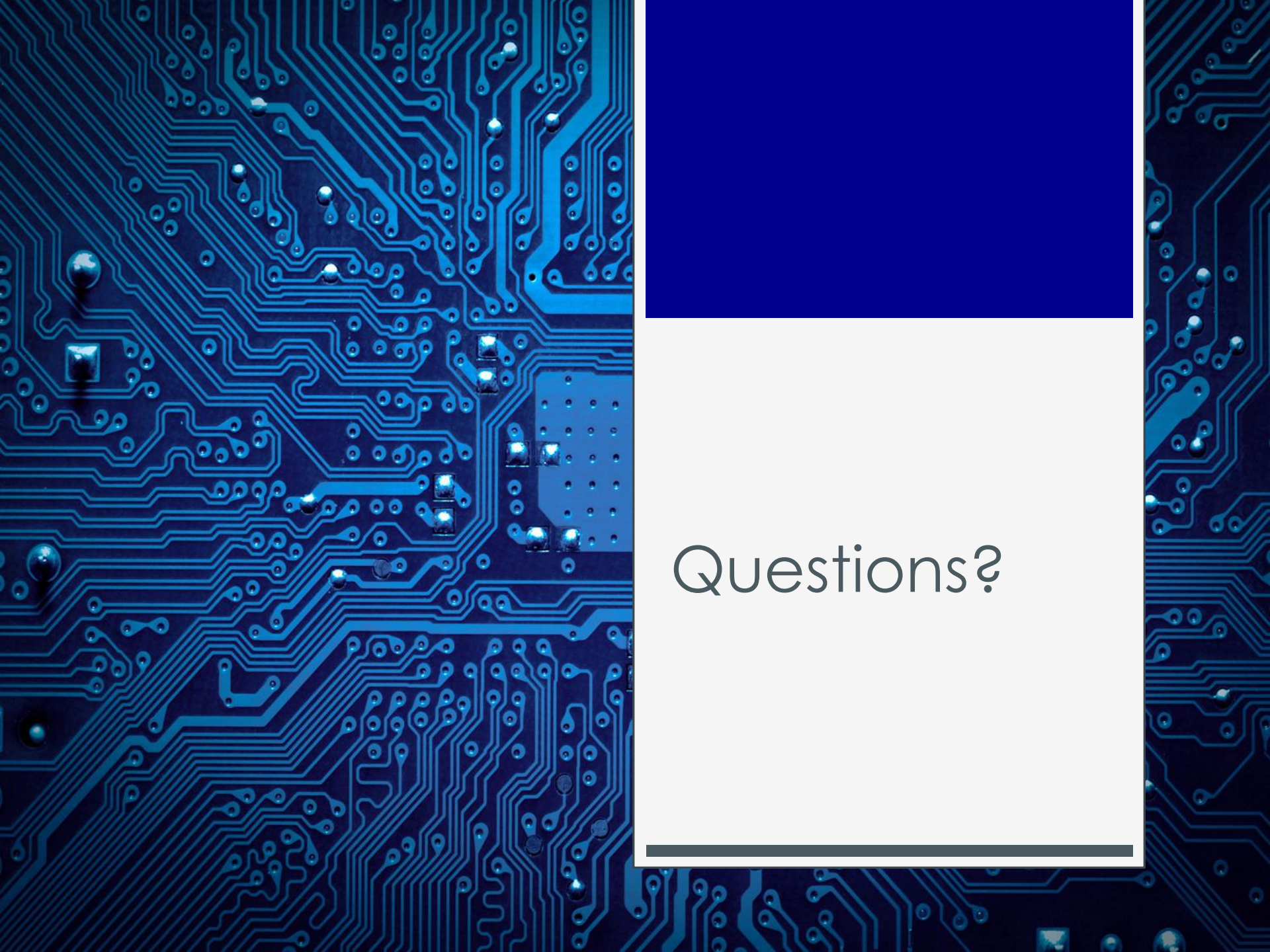
2) Alice sends a message X="Transfer $1000 to Mark" in the clear and Auth(X) to Bob. Mallory observes both messages and sends them to Bob a second time. Will Bob detect it?

3) Mallory and Alice both claim that they sent some message X with a valid Auth(X) to Bob. Can Bob know which of Alice or Mallory sent the message?

4) Bob claims that he received a message X with a valid Auth(X) from Alice (e.g., "Transfer $1000 from Alice to Bob") but Alice claims that she never sent it. Can Alice's claim be checked?

# Buffer Overflow

Typical buffer overflow attacks use the fact that the return address is at a **higher** memory address than the local variables (*i.e.*, the stack grows towards an address of 0). Explain how to carry out a buffer overflow attack if the stack layout is reversed (*i.e.*, the return address is at a lower memory address than the local variables).


Questions?