9 Security I (MGK)

A smartcard application requires a stack (LIFO) for storing data records. This stack can become much larger than the tiny amount of memory available on the card. Fortunately, the card terminal has enough memory, and its API offers a class `ExternalStack` that can be invoked remotely from the card. It offers the usual four methods: a constructor to initialise an empty stack, `push(`R`)` to place a data record R onto the stack, `isempty()` to test whether the stack contains no record, and `pop()` to remove and return the top record from the stack.

The integrity of the stack is crucial for the security of the application. However, the card terminal is not tamper resistant and the adversary may have full control over the `ExternalStack` object. Therefore, you have to implement a `SecureStack` wrapper class that uses `ExternalStack` as an untrusted storage provider while guaranteeing the integrity of any data returned. The trusted on-card memory available to a `SecureStack` object is only 256 bytes.

Consider how to implement on the card a class `SecureStack` that provides the same four methods by appending additional data to records before pushing them onto `ExternalStack`, and verifying any data returned against locally held values. You have a message authentication function `mac(`K`,(`R`,...))` and a cryptographic key/nonce generator function `gen()` available.

(*a*) Why is just appending a message authentication code to each externally stored record not sufficient? [2 marks]

(*b*) Write short pseudo-code for the four methods of `SecureStack` that shows how they call `ExternalStack`, how they update the on-card check data, and under which conditions a data-integrity alarm is raised. [10 marks]

(*c*) Express the internal check value(s) of your implementation after these calls:

```
Record r, r1, r2, r3;
SecureStack s;

s.push(r1);
s.push(r2);
r = s.pop();
s.push(r3);
```

[4 marks]

(*d*) Determine an upper limit for how often the `push` method of your implementation can be called securely. [4 marks]