Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

Symmetric encryption: Stream ciphers

Self-assessment test

Select the correct answer.

1. Stream ciphers…
   - Divide the message in quite big fragments and operate over each of them independently.
   - Require an external synchronization between the sender and the receiver.
   - Require a random and infinite keystream, ideally.
   - In practice the sender and receiver share a key whose length is that of the message.

2. Golomb postulates …
   - They set desirable properties that a keystream should meet.
   - They specify that the secret of the cipher should lie in the secret of the key.
   - They measure the quality (randomness) of the stream cipher output.
   - They point out, among other issues, that there should be no big number of identical consecutive symbols.

3. What for is the linear complexity useful?
   - To measure the unpredictability of a keystream.
   - To determine the speed of a LFSR.
   - To calculate the period of a keystream.
   - To estimate the necessary key length to reach a chosen security level.

4. A linear feed-back shift register (LFSR),
   - Allows the encryption of a value, or seed, using a XOR combination based on a polynomial.
   - Allows the generation of a sequence (for instance, a keystream) through an initial value.
   - Allows the generation of a binary no-periodic sequence.
   - They are highly secure systems due to their high lineal complexity.

5. Combining multiple LFSR…
    - The period of the generated sequence would be exponentially higher.
    - They generated sequence will be generated in a fast and secure way.
    - Compliance of Golomb postulates is guaranteed.
    - The lineal complexity of the system to generate the sequence (e.g. keystream) increases.

6. How many cells have a LFSR given by polynomial $p(x) = x^5 + x^3 + x^2 + 1$? How many inputs has its XOR?
    - 5 cells, 3 inputs
    - 4 cells, 4 inputs
    - 4 cells, 3 inputs
    - 3 cells, 3 inputs

7. In comparison with block ciphers, stream ciphers …
    - They are more appropriate for streaming-based systems.
    - They are more secure.
    - They are, on average, slower.
    - They generate more uncertainty for the cryptanalyst because the diffusion of the information is higher.

8. If the key is reused in several operations in a stream cipher…
    - If the cleartext is known, the encryption key could be achieved.
    - Any message could be decrypted if two or more cryptograms are obtained.
    - The key is disclosed immediately.
    - More speed is achieved without affected confidentiality.

9. Choose the correct sentence regarding RC4:
    - It uses a bidimensional matrix to store the internal state.
    - It is fast even in software implementations.
    - It uses a fixed key of 255 bytes.
    - It is currently unbreakable given the low linearity of its results.

10. Does RC4 algorithm use some encryption key?
    - No, just an internal state matrix
    - No, this is the reason why it is so fast.
    - Yes, to reorder the internal state.
    - Yes, to generate a random sequence with a LFSR.