Lecture 8

Random and Pseudorandom Numbers

When to use random numbers?

- Generation of a stream key for symmetric stream cipher
- Generation of keys for public-key algorithms
  - RSA public-key encryption algorithm (described in Chapter 3)
- Generation of a symmetric key for use as a temporary **session key**
  - used in a number of networking applications, such as Transport Layer Security (Chapter 5), Wi-Fi (Chapter 6), e-mail security (Chapter 7), and IP security (Chapter 8)
- In a number of key distribution scenarios
  - Kerberos (Chapter 4)

Two types of random numbers

- True random numbers:
    - generated in non-deterministic ways. They are not predictable and repeatable
- Pseudorandom numbers:
    - appear random, but are obtained in a deterministic, repeatable, and predictable manner

Properties of Random Numbers

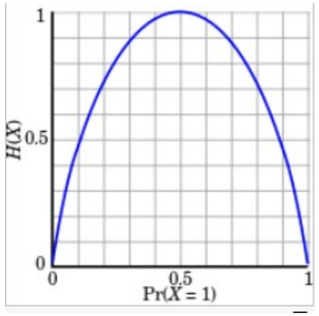
- Randomness
    - Uniformity
        - distribution of bits in the sequence should be uniform
    - Independence
        - no one subsequence in the sequence can be inferred from the others
- Unpredictable
    - satisfies the "next-bit test“

Entropy

- A measure of uncertainty
  - In other words, a measure of how unpredictable the outcomes are
  - High entropy = unpredictable outcomes = desirable in cryptography
  - The uniform distribution has the highest entropy (every outcome equally likely, e.g. fair coin toss)
  - Usually measured in bits (so 3 bits of entropy = uniform, random distribution over 8 values)

$$H = -\sum_{i} p_i \log_2(p_i)$$

Entropy of an information source


H(X)
Pr(X = 1)