Applied Cryptography
CPEG 472/672
Lecture 2A

Instructor: Nektarios Tsoutsos

What is random?

- Randomly generated bits
  - What is the randomness of the process?
- Common misconceptions
  - Mistaking non-randomness for randomness
    - Looks random so it must be random
  - Mistaking randomness for non-randomness
    - Patterns must be there for a reason

Probabilities

- Measures likelihood of an event occurring
- Uniform distribution
  - All outcomes are equally likely
  - Otherwise, it is non-uniform
- Fair coin
  - 0.5 probability of heads
- Biased coin
  - p probability of heads, 1-p probability of tails

Entropy

- Measures uncertainty
  - Amount of surprise in a result
  - Higher entropy => less certainty in a result
- Formula for entropy

$$-\sum p_i \cdot \log_2(p_i)$$

- Entropy of a fair coin

-(1/2)*log(1/2)-(1/2)*log(1/2)

RNGs and PRNGs

- In crypto we typically need
  - A source of entropy (RNG)
  - Algorithm to produce good random bits from the entropy source (PRNG)
- RNG sources
  - Device sensors, I/O, peripheral activity, logs, key presses, mouse etc.
- PRNGs can deterministically produce streams of reliable pseudorandom bits

PRNGs

- Run deterministic random bit generators
- Operations
  - Init the entropy pool, refresh (re-seed), next
- Security needs
  - Backtracking resistance
    - Cannot recover previously-generated bits
    - Need irreversible transformation in refresh and next operations
  - Prediction resistance
    - Cannot predict future bits
    - Call refresh regularly

Crypto vs non-crypto PRNGs

- Non-crypto PRNGs
  - Produce uniform distributions
  - Used in simulations etc.
  - Optimized for uniformity of distribution
  - Not concerned with predictability of bits
  - Must never be used for crypto
- Crypto-PRNGs
  - Are unpredictable
  - Produce well-distributed bits

Be careful

- PRNGs in programming languages are non-crypto
  - Always use known crypto-PRNGs
- Statistical tests != security
  - A weak crypto-PRNG can pass these tests
- If a PRNG is seeded with truly random bits, is it secure?
  - It can still leak its internal state

Reading for next lecture

- Aumasson: Chapter 2