Random and Pseudorandom Numbers

When to use random numbers?

Generate

- 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)

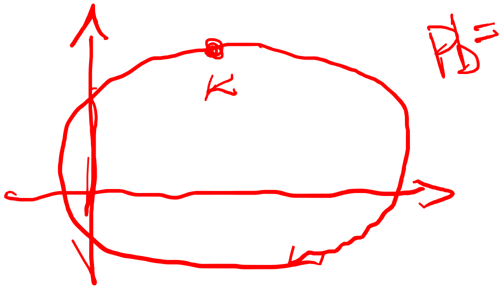
shared key
Symmetric key
temporary

- 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)

Https
TLS
Https.

- In a number of key distribution scenarios
  - Kerberos (Chapter 4)

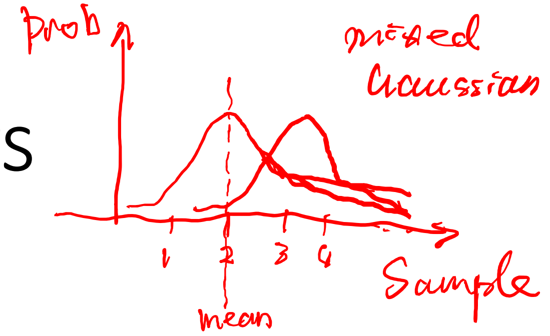
$P_B = K \cdot G$



Two types of random numbers

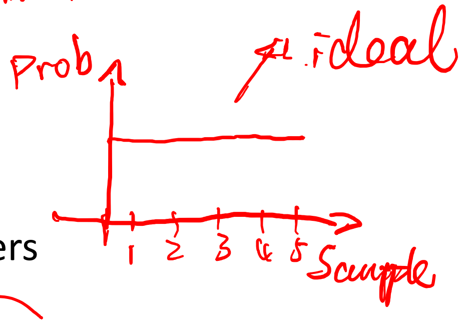
- True random numbers:
  - generated in non-deterministic ways. They are not predictable and repeatable
- Pseudorandom numbers:
  - appear random, but are obtained in a deterministic, repeatable, and predictable manner

Properties of Random Numbers



- Randomness
  - Uniformity
    - distribution of bits in the sequence should be uniform

why



  - Independence
    - no one subsequence in the sequence can be inferred from the others
- Unpredictable
  - satisfies the "next-bit test“

hop
old
new key

session key generation

any

sub sequence

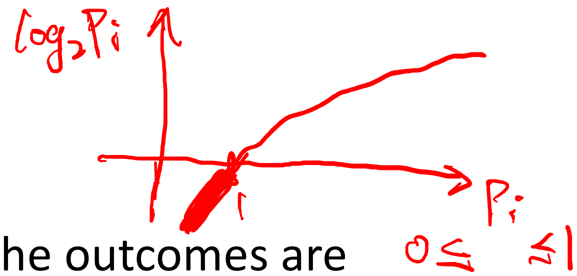
$P(AB) = P(A)\cdot P(B)$

independent

consecutive,

~~Mar~~ Markov Process

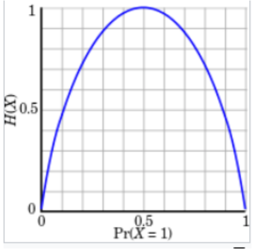
Entropy



- 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)

$$\overset{\text{entropy}}{H} = \overset{\geq 0}{-} \sum_i p_i \overset{< 0}{\boxed{\log_2 (\overset{\text{probability of value } i}{p_i})}}$$

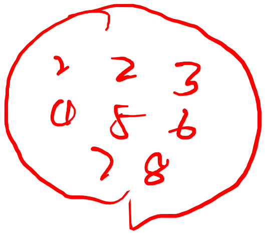
Entropy of an information source



$$H = -\sum_{i=1}^{n=8} P_i \log_2(P_i)$$

$$= -\left[\underbrace{\frac{1}{8}\cdot\log_2\frac{1}{8}}_{1\text{ value}} + \underbrace{0\cdot}_{\overset{0}{2\text{ values}}} + \underbrace{\frac{1}{16}\log_2\frac{1}{16}}_{3\text{ value}} + \cdots\cdots \underbrace{\frac{3}{16}\log_2\frac{3}{16}}_{8\text{ value}}\right]$$

data source random



value	prob
1	1/8
2	0
3	1/16
4	1/4
5	1/8
6	3/16
7	1/16
8	3/16