Introduction to Modern Cryptography

2nd lecture: Perfectly-Secure Encryption

some of these slides are copied from the University College London MSc InfoSec 2010 course given by Jens Groth
Thank you very much!
Finite Sets

- Sets $A = \{1,2\}$, $B = \{1,2,3,4\}$, $C = \{4\}$
- Empty set $\emptyset = \{}$
- Subsets/supersets $A \subseteq B$, $B \supseteq C$
- Intersection $A \cap B = \{1,2\}$
- Disjoint sets $A \cap C = \emptyset$
- Union $A \cup C = \{1,2,4\}$
- Relative complement $B \setminus A = \{3,4\}$
- Cartesian product $A \times C = \{(1,4),(2,4)\}$
- Cardinality $|A| = 2$, $|\emptyset| = 0$
- Rules $|A \cup B| = |A|+|B|-|A \cap B|$
Sample space, e.g. $\Omega = \{a, b, \ldots, z\}$

Probability mass function: $\Pr: \Omega \rightarrow [0, 1]$

$\Pr[a] + \Pr[b] + \ldots + \Pr[z] = 1$

Event $A \subseteq \Omega$

$\Pr[A] = \sum_{x \in A} \Pr[x]$

$\Pr[\emptyset] = 0 \quad \Pr[\Omega] = 1$

$0 \leq \Pr[A] \leq 1$
Probability Theory II

- If $A \subseteq B$ then $\Pr[A] \leq \Pr[B]$
- $\Pr[A \cap B] \leq \min(\Pr[A], \Pr[B])$
- $\max(\Pr[A], \Pr[B]) \leq \Pr[A \cup B] \leq \Pr[A] + \Pr[B]$
- $\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B]$
- $\Pr[A] - \Pr[B] \leq \Pr[A \setminus B] \leq \Pr[A]$
- independent events: $\Pr[A \cap B] = \Pr[A] \Pr[B]$
- conditional probabilities: For $B$ with $\Pr[B] > 0$ define $\Pr[A|B] := \Pr[A \cap B] / \Pr[B]$
- $A$ and $B$ are independent if and only if $\Pr[A|B] = \Pr[A]$
Random Variables (RV)

- Random variable: \( X: \Omega \to S \)
- Define \( \Pr[X = y] := \Pr[X^{-1}(y)] \)
- Joined random variables \( X: \Omega \to S, \ Y: \Omega \to T \) yields the random variable \( (X,Y): \Omega \to S \times T \)
- Independent random variables if for all \( x,y \)
  \( \Pr[(X,Y) = (x,y)] = \Pr[X = x] \Pr[Y = y] \)
Dependent RV

- $X: \Omega \to S, \quad Y: \Omega \to T$
- $\Pr[X=x | Y=y] = \Pr[(X,Y)=(x,y)] / \Pr[Y=y]$
- $\Pr[X=x, Y=y] = \Pr[X=x | Y=y] \Pr[Y=y]$
- Theorem:
  $\Pr[X=x] = \Pr[X=x | Y=y] \Pr[Y=y] + \Pr[X=x | Y\neq y] \Pr[Y\neq y]$
Gilbert Vernam
1890 – 1960

• engineer at AT&T Bell Labs
• inventor of stream cipher and one-time pad in 1919
• U.S. Patent 1,310,719
Frank Miller
1842 – 1918 or so

- banker in Sacramento, CA
- trustee of Stanford University
- invented one-time pad in 1882, 35 years earlier than Vernam!
One-Time Pad (OTP)

• Encryption:  
  \[ m = 101111 \]
  \[ k = 001010 \]
  \[ \text{Enc}_k(m) = c = m \oplus k = 100101 \]

• Decryption:  
  \[ c = 100101 \]
  \[ k = 001010 \]
  \[ \text{Dec}_k(c) = m = c \oplus k = 101111 \]
Problems with OTP

- key needs to be as long as message
- key can only be used once
- provides no authentication
- key has to be truly random
- more info on wikipedia, another source
Claude Elwood Shannon
1916 - 2001

- Father of Information Theory
- Graduate of MIT
- Bell Labs
- juggling, unicycling, chess
- ultimate machine