Introduction to Modern Cryptography

2nd lecture (today):

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!

last week:

- introduction
- historical ciphers
- discrete probabilities

2nd lecture (today):

- 3 principles of Modern Crypto
- Perfectly-Secure Encryption

Jonathan Katz

Yehuda Lindell

- 3 Basic Principles of Modern Cryptography

1. Formulation of Exact Definitions

- "a cryptographic scheme is secure if no adversary of a specified power can achieve a specified break"
  example: encryption
- mathematical definitions vs the real world
  example: power-usage attacks
- cryptographers face a similar problem as Turing: "Am I modeling the right thing?"

2. Reliance on Precise Assumptions

- unconditional security is often impractical (unfortunate state of computational complexity)
- validation of assumptions (independent of cryptography)
  example: factoring
- allows to compare crypto schemes

3. Rigorous Proofs of Security

- Intuition is not good enough. History knows countless examples of broken schemes
- bugs vs security holes
  software users vs adversaries
- reduction proofs: Given that Assumption X is true, Construction Y is secure.
  Any adversary breaking Construction Y can be used as subroutine to violate Assumption X.

Finite Sets

- Sets $A = \{1,2\}$ $B = \{1,2,3,4\}$ $C = \{4\}$
- Empty set $\varnothing = \{\}$
- Subsets/supersets $A \subseteq B$, $B \supseteq C$
- Intersection $A \cap B = \{1,2\}$
- Disjoint sets $A \cap C = \varnothing$
- Union $A \cup C = \{1,2,4\}$
- Relative complement $B \setminus A = \{3,4\}$
- Cartesian product $A \times C = \{(1,4),(2,4)\}$
- Cardinality $|A| = 2$, $|\varnothing| = 0$
- Rules $|A \cup B| = |A|+|B|-|A \cap B|$

Probability Theory

- Sample space, e.g. $\Omega = \{a,b,\ldots,z\}$
- Probability mass function: $\Pr: \Omega \to [0,1]$
- $\Pr[a] + \Pr[b] + \ldots + \Pr[z] = 1$
- Event $A \subseteq \Omega$
- $\Pr[A] = \sum_{x \in A} \Pr[x]$
- $\Pr[\emptyset] = 0$ $\Pr[\Omega] = 1$
- $0 \leq \Pr[A] \leq 1$

Probability Theory II

- If $A \subseteq B$ then $\Pr[A] \le \Pr[B]$
- $\Pr[A \cap B] \le \min(\Pr[A], \Pr[B])$
- $\max(\Pr[A], \Pr[B]) \le \Pr[A \cup B] \le \Pr[A] + \Pr[B]$
- $\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B]$
- $\Pr[A] - \Pr[B] \le \Pr[A \setminus B] \le \Pr[A]$
- 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 $\Pr[A|B] = \Pr[A]$

union bound

Random Variables (RV)

- Random variable: $X: \Omega \to S$
- Define $\Pr[X = y] := \Pr[\, X^{-1}(y) \,]$
- Joined random variables
  $$X: \Omega \to S, \quad Y: \Omega \to T$$
  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

- $X: \Omega \to S, \quad Y: \Omega \to T$
- $\Pr[X=x \mid Y=y] = \Pr[(X,Y)=(x,y)] / \Pr[Y=y]$
- $\Pr[X=x, Y=y] = \Pr[X=x \mid Y=y] \Pr[Y=y]$
- Theorem:
  $\Pr[X=x] =$
  $\Pr[X=x \mid Y=y] \Pr[Y=y] + \Pr[X=x \mid Y \neq y] \Pr[Y \neq y]$

RISC seminar

- you are invited to join the RISC mailing list
- and attend the next RISC seminar
- https://projects.cwi.nl/crypto/TOC2014/

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:

$$\begin{array}{rl} m & = 101111 \\ k & = 001010 \\ \hline \mathrm{Enc}_k(m) = c = \quad m \oplus k & = 100101 \end{array}$$

- Decryption:

$$\begin{array}{rl} c & = 100101 \\ k & = 001010 \\ \hline \mathrm{Dec}_k(c) = m = \quad c \oplus k & = 101111 \end{array}$$

Problems with OTP

- key needs to be as long as message
- key can only be used once, see here why
- 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