Models and analysis of security protocols
1st Semester 2011-2012
Introduction
Lecture 1

Pascal Lafourcade

Université Joseph Fourier, Verimag

Master 2 Pro: September 2011
Instructors

- Pascal Lafourcade: pascal.lafourcade@imag.fr
- Martin Gagné: martin.gagne@imag.fr
- Jean-Louis Roch: jean-louis.roch@imag.fr
- Florent Autreau: florent.autreau@imag.fr
Administrative Informations

Where & When

- Module of 24 sessions + 16
  - 12 sessions + 3 with JL Roch
  - 12 sessions + 3 with P Lafourcade
  - other sessions with F Autreau
Draft of my Lecture Schedule

1. 26th September Introduction and Probability
2. 26th September Indistinguishability and Security Notions
3. 3th October Reduction Proofs
4. 3th October Hybrid Argument
5. 3th October Symmetric Encryption
6. 31th October Security of Protocols
7. 31th October Passive Intruder
8. 7th November Active Intruder
9. 14th November Tools and Application
10. 21th November Access Control
11. 21th November Non Interference and Others
12. 28th November Link Between Computational and Symbolic

3 exercises sessions are planned by Martin

▷ 5th October 2010
▷ 3th November 2010
▷ 24th and 29th November 2010
Evaluation Informations

Exams

- Mid-term Exam
- Exam
- Evaluation:
  - ET: Final examination: 1 written exam (3h)
  - TP: Practical work: 1 session
  - CC: Continuous controls: written control and one lecture report (Friday in November 2011).
- Final mark: 20% * TP + 65% * ET + 15% * MAX(ET,CC)
Possible Articles

1. On Some Incompatible Properties of Voting Schemes
2. A Generalization of DDH with Applications to Protocol Analysis and Computational Soundness.
3. Public-key Encryption in a Multi-User Setting: Security Proofs and Improvements
4. Cryptographic Hash-Function Basics
5. Using Hash Functions as a Hedge against Chosen Ciphertext Attack
6. Stateful Public-Key Cryptosystems: How to Encrypt with One 160-bit Exponentiation
7. A multiplicative homomorphic sealed-bid auction based on goldwasser-micali encryption
8. Declassification: Dimensions and principles
9. A Concrete Security Treatment of Symmetric Encryption by
Organization

### Timetable and Rooms

Monday or Thursday
- 8h-9h30
- 9h45-11h15
- 11h15-12h45h

During each lecture, some students will take some notes, and produce a latex file for the next week. REGISTRATION NOW.
Registration ASAP

- Lecture 1, scribes are:
- Lecture 2, scribes are:
- Lecture 3, scribes are:
- Lecture 4, scribes are:
- Lecture 5, scribes are:
- Lecture 6, scribes are:
- Lecture 7, scribes are:
- Lecture 8, scribes are:
- Lecture 9, scribes are:
- Lecture 10, scribes are:
- Lecture 11, scribes are:
- Lecture 12, scribes are:

Group of 2 or 3
Instructor Information (I)

Address

- Instructor: Pascal Lafourcade
- Address:
  
  VERIMAG, team DCS  
  Center Equation CTL  
  2, avenue de Vignate  
  38610 Gières  

- Email: pascal.lafourcade@imag.fr  
- Web: http://www-verimag.imag.fr/~plafourc/  
- Phone: +33 (0) 4 56 52 04 14 (but email is better)  
- Available most of the time in my office by appointment
### Instructor Information (II)

<table>
<thead>
<tr>
<th>Research in:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security, Formal Verification, Cryptographic Protocols,</td>
</tr>
<tr>
<td>Rewriting, Unification, Equational Theories, Constraints:</td>
</tr>
<tr>
<td>▶ e-voting</td>
</tr>
<tr>
<td>▶ e-auction</td>
</tr>
<tr>
<td>▶ Group protocols</td>
</tr>
<tr>
<td>▶ Wireless communications</td>
</tr>
<tr>
<td>▶ Tools</td>
</tr>
<tr>
<td>▶ Automatic verification</td>
</tr>
<tr>
<td>▶ protocols</td>
</tr>
<tr>
<td>▶ cryptosystems</td>
</tr>
<tr>
<td>▶ …</td>
</tr>
</tbody>
</table>


Web Pages

Courses Web Pages:

- Practical Informations online.
- Slides, homework, references, articles...

Unit part:  http://www-id.imag.fr/Laboratoire/Membres/Roch_Jean-Louis/perso_html/COURS/KIOSK-SCCI-SecurityModels/

My part:

www-verimag.imag.fr/~plafourc/teaching/Master_Pro_2_2011_2012.php
## Prerequisites

Some familiarity with computer system:

- operating systems,
- networks,
- programming languages.

Some mathematical notions:

- a little number theory,
- some probability notions,
- ability to follow and do proofs, e.g., proof by induction, contradiction...
- acquaintance with logic,
- ease with formal notation and manipulation,

but no advanced mathematics required.

Please see me if you have any doubt or question.
What is this course about?

A Master 2nd year course.

A presentation to basics and essential notions, techniques, models used in security and cryptography.

A look at some more advanced topics in cryptography, in particular topics related to the link between mathematical point of view and computer science one.
Contents (I)

Security touches many domains:

▶ cryptography,
▶ mathematics,
▶ operating system,
▶ networking,
▶ economics,
▶ policy and law ...

We should at least touch most of these topics, but we will not try to cover all aspects of security.
Contents (II)

- Not a course on cryptography,
- Not a complete course on security.
Course topics, in details

1. Introduction & Probability
2. Indistinguishability and Security Notions OW, IND, NM, CPA, CCA, Hard Problem DDH, CDH ....
3. Reduction Proofs
4. Hybrid Argument
5. Security of Symmetric encryption and OAEP
6. Security of protocols in the Symbolic Model
7. Passive Intruder
8. Active Intruder
9. Tools and Applications
10. Access Control and Security Policies
11. Non-interference, and others
12. Link between Computational and Symbolic

And a little more, if possible...

Today: Introduction + Indistinguishability
Reading

Required reading:

- No textbook!
- Many papers, indicated during the course.

Some recommended book:

- Two volumes of: “The Foundations of Cryptography” by Oded Goldreich
- Jonathan Katz and Yehuda Lindell “Introduction to modern cryptography”
More books

- Bruce Schneier “Applied cryptography”,
- Douglas Stinson “Cryptography: Theory and Practice”,
Course work

- Reading.
- Class participation.
- Homework:
  - Prepare IT
  - Given and explained in class,
  - Presentation of exercise on blackboard
- Latex file summarizing previous lecture.
- Exam.
Cheating (I)

- All work you make must be your own!
- If you do not know if something is allowed, please ask.
- Cheating will result in failure of the course and other standard measures.

Regular class attendance is required!
Cheating (II)

➤ You are encouraged to discuss the course material and assignments with others.
➤ You are not allowed to do assignments with others
➤ You may use any conversations, texts, or other material, as long as you cite your sources.
Outline

Presentation

Motivations

Probabilities

Conclusion
Traditional security properties

▶ Common security properties are:
  - **Confidentiality or Secrecy**: No improper disclosure of information
  - **Authentication**: To be sure to talk with the right person.
    disclosure of information
  - **Integrity**: No improper modification of information
  - **Availability**: No improper impairment of functionality/service
Authentication

"On the Internet, nobody knows you're a dog."
Mechanisms for Authentication

1. Something that you know
   E.g. a PIN or a password

2. Something that you have
   E.g. a smart-card

3. Something that you are
   Biometric characteristics like voice, fingerprints, eyes, ...

4. Where you are located
   E.g. in a secure building

Strong authentication combines multiple factors:
E.g., Smart-Card + PIN
Other security properties

- **Non-repudiation** (also called **accountability**) is where one can establish responsibility for actions.

- **Fairness** is the fact there is no advantage to play one role in a protocol comparing with the other ones.

- **Privacy**
  - **Anonymity**: secrecy of principal identities or communication relationships.
  - **Pseudonymity**: anonymity plus link-ability.
  - **Data protection**: personal data is only used in certain ways.
Example: banking

- A bank may require
  - authenticity of clients (at teller, ATMs, or on the Internet),
  - non-repudiation of transactions,
  - integrity of accounts and other customer data,
  - secrecy of customer data, and
  - availability of logging.

- The conjunction of these properties might constitute the bank’s (high-level) security policy.
Another example: e-voting

- An e-voting system should ensure that
  - only registered voters vote,
  - each voter can only vote once,
  - integrity of votes,
  - privacy of voting information (only used for tallying), and
  - availability of system during voting period

- In practice, many policy aspects are difficult to formulate precisely.

Exercise: Give the security properties that an international airport should guarantee.
More details with Florent Autreau later.
Outline

Presentation

Motivations

Probabilities
  Mathematics Recalls
  Birthday Paradox
  Negligible Functions

Conclusion
Outline

Presentation

Motivations

Probabilities

Mathematics Recalls

Birthday Paradox

Negligible Functions

Conclusion
Probability Distribution (I)

A finite probability distribution \( D = (U, P) \) is:
a finite, non-empty set \( U \), together with a function \( P \) that maps \( u \in U \) to \( P[u] \in [0, 1] \), such that

\[
\sum_{u \in U} P[u] = 1
\]

The set \( U \) is called the sample space and the function \( P \) is called the probability function.

Example

If we think of rolling a fair die, then \( U := \{1, 2, 3, 4, 5, 6\} \), and \( P[u] := 1/6 \) for all \( u \in U \) gives a probability distribution describing the possible outcomes of the experiment.
Probability Distribution (II)

An event is a subset $A$ of $U$, and the probability of $A$ is:

$$P[A] := \sum_{u \in A} P[u]$$

Properties

For an event $A \subseteq U$, let $\overline{A}$ denote the complement of $A$ in $U$.

$$P[\emptyset] = 0, \quad P[U] = 1, \quad P[\overline{A}] = 1 - P[A]$$

For any events $A, B \subseteq U$, if $A \subseteq B$, then $P[A] \leq P[B]$. Also, for any events $A, B \subseteq U$, we have


in particular, if $A$ and $B$ are disjoint, then $P[A \cup B] = P[A] + P[B]$. 
Probability Distribution (III)

More generally, for any events \( A_1, \ldots, A_n \subseteq U \) we have

\[
P[A_1 \cup \ldots \cup A_n] \leq P[A_1] + \ldots + P[A_n]
\]

and if the \( A_i \) are pairwise disjoint, then

\[
P[A_1 \cup \ldots \cup A_n] = P[A_1] + \ldots + P[A_n]
\]

DeMorgan’s law

Let \( A \) and \( B \) two events, we have:

- \( \overline{A \cup B} = \overline{A} \cap \overline{B} \)
- \( \overline{A \cap B} = \overline{A} \cup \overline{B} \)

Distributive law

For events \( A, B, C \), we have:

- \( A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \)
- \( A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \)
Conditional distribution

Let $D = (U, P)$ be a probability distribution. For any event $B \subseteq U$ with $P[B] \neq 0$ and any $u \in U$, let us define:

$$P[u|B] := \begin{cases} \frac{P[u]}{P[B]} & \text{if } u \in B, \\ 0 & \text{otherwise} \end{cases}$$

For any event $A \subseteq U$, we have

$$P[A|B] = \sum_{u \in A} P[u|B] = \frac{P[A \cap B]}{P[B]}$$

value $P[A|B]$ is called the **conditional probability** of $A$ given $B$. 


Theorem: Bayes

Suppose we have a collection $B_1, \ldots, B_n$ of events that partitions $U$, such that each event $B_i$ occurs with non-zero probability. Then it is easy to see that for any event $A$,

$$P[A] = \sum_{i=1}^{n} P[A \cap B_i] = \sum_{i=1}^{n} P[A|B_i]P[B_i]$$

Furthermore, if $P[A] \neq 0$, then for any $j = 1, \ldots, n$, we have:

$$P[B_j|A] = \frac{P[A \cap B_j]}{P[A]} = \frac{P[A|B_j]P[B_j]}{\sum_{i=1}^{n} P[A|B_i]P[B_i]}$$

This equality, known as Bayes’ theorem, lets us compute the conditional probability $P[B_j|A]$ in terms of the conditional probabilities $P[A|B_i]$. 
Bayes Example: Cookies

<table>
<thead>
<tr>
<th></th>
<th>Bowl 1</th>
<th>Bowl 2</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chocolate Chip</td>
<td>10</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>Plain</td>
<td>30</td>
<td>20</td>
<td>50</td>
</tr>
<tr>
<td>Total</td>
<td>40</td>
<td>40</td>
<td>80</td>
</tr>
</tbody>
</table>

Figure: Number of cookies in each bowl by type of cookie

Fred picks a bowl at random, and then picks a cookie at random.

What is the probability that Fred has a plain cookie, given that he has picked bowl 1?

The cookie turns out to be a plain one. How probable is it that Fred picked it out of bowl 1?
Cookies Answer (I)

<table>
<thead>
<tr>
<th></th>
<th>Bowl 1</th>
<th>Bowl 2</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chocolate Chip</td>
<td>1/8</td>
<td>1/4</td>
<td>3/8</td>
</tr>
<tr>
<td>Plain</td>
<td>3/8</td>
<td>1/4</td>
<td>5/8</td>
</tr>
<tr>
<td>Total</td>
<td>1/2</td>
<td>1/2</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure: Relative frequency of cookies in each bowl by type of cookie

- $Pr(A)$ = the probability that Fred picked bowl 1 regardless of any other information. Hence $Pr(A) = 1/2$
- $Pr(B)$ = the probability of getting a plain cookie regardless of any information on the bowls.
  - $Pr(B) = 3/8 + 1/4 = 0.625$
  - $Pr(B) = 50/80 = 0.625$
- $Pr(B|A)$ = the probability of getting a plain cookie given that Fred has selected bowl 1. $Pr(B|A) = 30/40 = 0.75$
Cookies Answer (II)

Given all this information, we can compute the probability of Fred having selected bowl 1 given that he got a plain cookie, as such:

\[
P(A|B) = \frac{P(B|A)P(A)}{P(B)} = \frac{0.75 \times 0.5}{0.625} = 0.6
\]

As we expected, it is more than half.
Exercise: Drug Test

Suppose a certain drug test is 99% accurate, that is, the test will correctly identify a drug user as testing positive 99% of the time, and will correctly identify a non-user as testing negative 99% of the time. Let’s assume a corporation decides to test its employees for opium use, and 0.5% of the employees use the drug.

We want to know the probability that, given a positive drug test, an employee is actually a drug user.
Random variables

Let \( D = (U, P) \) be a probability distribution. A random variable \( X \) is a function from \( U \) into a set \( \mathcal{X} \). If \( \mathcal{X} \) is a subset of the real numbers, then \( X \) is called a real random variable: \( X(U) = \{X(u) : u \in U\} \).

Properties

If \( X : U \rightarrow \mathcal{X} \) is a random variable, and \( f : \mathcal{X} \rightarrow Y \) is a function, then \( f(X) := f \circ X \) is also a random variable.

Let \( X : U \rightarrow \mathcal{X} \) be a random variable. For \( x \in \mathcal{X} \), we write "\( X = x \)" as shorthand for the event \( \{u \in U : X(u) = x\} \).
Independent Random Variables

Definition

Two random variables $X, Y$ are independent if for all $x$ in the image of $X$ and all $y$ in the image of $Y$, the events $X = x$ and $Y = y$ are independent:

$$P[X = x \land Y = y] = P[X = x]P[Y = y]$$

Equivalently, $X$ and $Y$ are independent if and only if their joint distribution is equal to the product of their individual distributions.

Exercise: Prove that $X$ and $Y$ are independent if and only if for all values $x$ taken by $X$ with non-zero probability, the conditional distribution of $Y$ given the event $X = x$ is the same as the distribution of $Y$.
Pairwise Independent Random Variables

Let $X_1, ..., X_n$ be a collection of random variables, and let $X_i$ be the image of $X_i$ for $i = 1, ..., n$. We say $X_1, ..., X_n$ are **pairwise independent** if for all $i, j = 1, ..., n$ with $i \neq j$, the variables $X_i$ and $X_j$ are independent.
Mutually Independent Random Variables

We say that $X_1, \ldots, X_n$ are mutually independent if for all $x_1 = X_1, \ldots, x_n = X_n$, we have

$$P[X_1 = x_1 \land \ldots \land X_n = x_n] = \prod_{i=1}^{n} P[X_i = x_i]$$

More generally, for $k = 2, \ldots, n$, we say that $X_1, \ldots, X_n$ are $k$-wise independent if any $k$ of them are mutually independent.
Example

We toss three coins, and set $X_i := 0$ if the $i$th coin is "tails," and $X_i := 1$ otherwise.

Show that the variables $X_1, X_2, X_3$ are mutually independent.

Let us set $Y_{12} := X_1 \oplus X_2$, $Y_{13} := X_1 \oplus X_3$, and $Y_{23} := X_2 \oplus X_3$, where "$\oplus$" denotes "exclusive or," that is, addition modulo 2.

Show that the variables $Y_{12}, Y_{13}, Y_{23}$ are pairwise independent, but not mutually independent.
Probability Notation

\[ Pr[A(X_n) = 1] = \sum_x Pr[X_n = x].Pr[A(x) = 1] \]
Expectation

Let $D = (U, P)$ be a probability distribution. If $X$ is a real random variable, then its **expected value** is:

$$E[X] := \sum_{u \in U} X(u)P[u]$$

**Properties**

If $\mathcal{X}$ is the image of $X$, we have:

$$E[X] = \sum_{x \in \mathcal{X}} \sum_{u \in X^{-1}(x)} xP[u] = \sum_{x \in \mathcal{X}} xP[X = x]$$

More generally,

$$E[f(X)] = \sum_{x \in \mathcal{X}} f(x)P[X = x]$$
Examples

Let $X$ be uniformly distributed over $\{1, \ldots, n\}$.

$$E[X] = \sum_{x=1}^{n} x \cdot \frac{1}{n} = \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2}$$

Let $X$ denote the value of a die toss. Let $A$ be the event that $X$ is even. $X$ is uniformly distributed over $\{2, 4, 6\}$, and hence

$$E[X|A] = \frac{2 + 4 + 6}{3} = 4$$

Similarly, in the conditional probability space given $\bar{A}$, we see that $X$ is uniformly distributed over $\{1, 3, 5\}$, and hence

$$E[X|\bar{A}] = \frac{1 + 3 + 5}{3} = 3$$

Hence

$$E[X] = E[X|A]P[A] + E[X|\bar{A}]P[\bar{A}] = 4 \cdot \frac{1}{2} + 3 \cdot \frac{1}{2} = \frac{7}{2}$$
Properties

First, if $X$ is equal to a constant $c$ (i.e., $X(u) = c$ for all $u \in U$), then $E[X] = E[c] = c$.

Second, if $X$ takes only non-negative values (i.e., $X(u) \geq 0$ all $u \in U$), then $E[X] \geq 0$. Similarly, if $X$ takes only positive values, then $E[X] > 0$.

Linearity of expectation

For real random variables $X$ and $Y$, and real number $a$, we have $E[X + Y] = E[X] + E[Y]$ and $E[aX] = aE[X]$.

If $X$ and $Y$ are independent real random variables, then $E[XY] = E[X]E[Y]$.

Exercise: Proofs
Variance

The **variance** of a real random variable $X$ is

$$Var[X] := E[(X - E[X])^2]$$

It is a measure of the spread or dispersion of the distribution of $X$ around its expected value $E[X]$. Variance is always non-negative.

**Properties**

Let $X$ be a real random variable, and let $a$ and $b$ be real numbers. Then we have:

- $Var[X] = E[X^2] - (E[X])^2$
- $Var[aX] = a^2 Var[X]$
- $Var[X + b] = Var[X]$

**Exercise:** Proofs
Examples

Let $X$ be uniformly distributed over \{1, ..., $n$\}.

$$E[X] = \sum_{x=1}^{n} x \cdot \frac{1}{n} = \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2}$$

We also have

$$E[X^2] = \sum_{x=1}^{n} x^2 \cdot \frac{1}{n} = \frac{n(n+1)(2n+1)}{6} \cdot \frac{1}{n} = \frac{(n+1)(2n+1)}{6}$$

Therefore,

$$Var[X] = E[X^2] - (E[X])^2 = \frac{n^2 - 1}{12}$$
Theorem: Markov’s inequality

Let $X$ be a random variable that takes only non-negative real values. Then for any $t > 0$, we have

$$P[X \geq t] \leq \frac{E[X]}{t}$$

Exercise: Proof
Theorem Chebyshev’s inequality

Let $X$ be a real random variable. Then for any $t > 0$, we have:

$$P[|X - E[X]| \geq t] \leq \frac{Var[X]}{t^2}$$

Exercise: Proof
Theorem: Chernoff bound

Let $X_1, ..., X_n$ be mutually independent random variables, such that each $X_i$ is 1 with probability $p$ and 0 with probability $q := 1 - p$. Assume that $0 < p < 1$. Also, let $X$ be the sample mean of $X_1, ..., X_n$. Then for any $\epsilon > 0$, we have:

$$P[\bar{X} - p \geq \epsilon] \leq e^{-n\epsilon^2/2qp}$$
$$P[\bar{X} - p \leq -\epsilon] \leq e^{-n\epsilon^2/2p}$$
$$P[|\bar{X} - p| \geq \epsilon] \leq 2e^{-n\epsilon^2/2}$$

Exercise: Proof
Outline

Presentation

Motivations

Probabilities

Mathematics Recalls

Birthday Paradox

Negligible Functions

Conclusion
Birthday Paradox: My bet

When are you born?
Birthday Paradox & Probabilities (I)

- How many people must be in a room such that the probability $p$ that one has your birthday is $p > 0.5$?
Birthday Paradox & Probabilities (I)

- How many people must be in a room such that the probability $p$ that one has your birthday is $p > .5$?
- In a room of $n$ people the probability is $1 - \left(\frac{365-1}{365}\right)^n$. 
Birthday Paradox & Probabilities (I)

- How many people must be in a room such that the probability $p$ that one has your birthday is $p > .5$?
- In a room of $n$ people the probability is $1 - \left(\frac{365-1}{365}\right)^n$.
- So we have:

$$n \geq \frac{\ln\left(\frac{1}{2}\right)}{\ln\left(\frac{365-1}{365}\right)} \approx 252, 651 \approx 253$$
Birthday Paradox & Probabilities (II)

- How many people must be in a room such that the probability $p$ that any two share the same birthday is $p > .5$?
Birthday Paradox & Probabilities (II)

How many people must be in a room such that the probability \( p \) that any two share the same birthday is \( p > 0.5 \)?

As stated above, the probability that no two birthdays coincide is

\[
1 - p(n) = \bar{p}(n) = \prod_{k=1}^{n-1} \left( 1 - \frac{k}{365} \right)
\]

Hence \( n \geq 23 \) persons!
Birthday Paradox & Probabilities (II)

- How many people must be in a room such that the probability $p$ that any two share the same birthday is $p > .5$?

- As stated above, the probability that no two birthdays coincide is

$$1 - p(n) = \bar{p}(n) = \prod_{k=1}^{n-1} \left(1 - \frac{k}{365}\right)$$

- Using the inequality $1 + x < e^x$

$$\bar{p}(n) = \prod_{k=1}^{n-1} \left(1 - \frac{k}{365}\right) < \prod_{k=1}^{n-1} \left(e^{-k/365}\right) = e^{-(n(n-1))/(2 \cdot 365)}$$

$$e^{-(n(n-1))/(2 \cdot 365)} < \frac{1}{2}, \text{ we get } n^2 - n > 2 \cdot 365 \ln 2$$
Birthday Paradox & Probabilities (II)

► How many people must be in a room such that the probability $p$ that any two share the same birthday is $p > .5$?

► As stated above, the probability that no two birthdays coincide is

$$1 - p(n) = \overline{p}(n) = \prod_{k=1}^{n-1} \left( 1 - \frac{k}{365} \right)$$

► using the inequality $1 + x < e^x$

$$\overline{p}(n) = \prod_{k=1}^{n-1} \left( 1 - \frac{k}{365} \right) < \prod_{k=1}^{n-1} \left( e^{-k/365} \right) = e^{-(n(n-1))/(2 \cdot 365)}$$

$$e^{-(n(n-1))/(2 \cdot 365)} < \frac{1}{2}, \text{ we get } n^2 - n > 2 \cdot 365 \ln 2$$

► Hence $n \geq 23$ persons!
Birthday Paradox

\[ A_n = \{ \text{At least two of the } n \text{ people share a birthday} \} \]

<table>
<thead>
<tr>
<th>n</th>
<th>An</th>
<th>n</th>
<th>An</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.00000000</td>
<td>16</td>
<td>0.28360400</td>
</tr>
<tr>
<td>2</td>
<td>0.00273972</td>
<td>17</td>
<td>0.31500766</td>
</tr>
<tr>
<td>3</td>
<td>0.00820416</td>
<td>18</td>
<td>0.34691141</td>
</tr>
<tr>
<td>4</td>
<td>0.01635591</td>
<td>19</td>
<td>0.37911852</td>
</tr>
<tr>
<td>5</td>
<td>0.02713557</td>
<td>20</td>
<td>0.41143838</td>
</tr>
<tr>
<td>6</td>
<td>0.04046248</td>
<td>21</td>
<td>0.44368833</td>
</tr>
<tr>
<td>7</td>
<td>0.05623570</td>
<td>22</td>
<td>0.47569530</td>
</tr>
<tr>
<td>8</td>
<td>0.07433529</td>
<td>23</td>
<td>0.50729723</td>
</tr>
<tr>
<td>9</td>
<td>0.09462383</td>
<td>24</td>
<td>0.53834425</td>
</tr>
<tr>
<td>10</td>
<td>0.11694817</td>
<td>25</td>
<td>0.56869970</td>
</tr>
<tr>
<td>11</td>
<td>0.14114137</td>
<td>26</td>
<td>0.59824082</td>
</tr>
<tr>
<td>12</td>
<td>0.16702478</td>
<td>27</td>
<td>0.62685928</td>
</tr>
<tr>
<td>13</td>
<td>0.19441027</td>
<td>28</td>
<td>0.65446147</td>
</tr>
<tr>
<td>14</td>
<td>0.22310251</td>
<td>29</td>
<td>0.68096853</td>
</tr>
<tr>
<td>15</td>
<td>0.25290131</td>
<td>30</td>
<td>0.70631624</td>
</tr>
</tbody>
</table>
Birthday Paradox
Hash Functions

A hash function $\mathcal{H}$ takes as input a bit-string and returns a corresponding 'digest' of fixed length. Good hash functions are:

- **collision-free**: $\mathcal{H}(x) = \mathcal{H}(y) \Rightarrow x = y$
- **non-malleable**: $x \not\sim R y \not\Rightarrow \mathcal{H}(x) \not\sim R \mathcal{H}(y)$

$\mathcal{H}(Alice) = \not= \mathcal{H}(Bob)$
## Properties of hash functions

### Definition (Preimage resistance)

Given an output $y$, it is computationally infeasible to compute $x$ such that

$$h(x) = y$$

### Definition (2nd Preimage resistance)

Given an input $x$, it is computationally infeasible to compute $x'$ such that

$$h(x') = h(x)$$
Properties of hash functions

**Definition (Collision resistance)**

It is computationally infeasible to compute \( x \) and \( x' \) such that

\[
h(x) = h(x')
\]
Properties of hash functions

Alternate terminology:

- *pre-image resistant* $\equiv$ *one-way*
- *2nd pre-image resistant* $\equiv$ *weak collision resistant*
- *collision resistant* $\equiv$ *strong collision resistant*
Use of hash functions

Idea: compute a condensed message $y$ from a given message $m$. The condensed should be specific to the message.

- Use $y$ in place of $m$ in a trustworthy way.
- "Did you get $m$ correctly? Here’s $y$ to check." (file-sharing)
- "Could you decrypt $c$ correctly?"
- "I sign $y$ to prove that I wrote $m$."
List of Hash Functions

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Output size</th>
<th>Internal state size</th>
<th>Block size</th>
<th>Length size</th>
<th>Word size</th>
<th>Collision</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAVAL</td>
<td>256/…/128</td>
<td>256</td>
<td>1024</td>
<td>64</td>
<td>32</td>
<td>Yes</td>
</tr>
<tr>
<td>MD2</td>
<td>128</td>
<td>384</td>
<td>128</td>
<td>No</td>
<td>8</td>
<td>Almost</td>
</tr>
<tr>
<td>MD4</td>
<td>128</td>
<td>128</td>
<td>512</td>
<td>64</td>
<td>32</td>
<td>Yes</td>
</tr>
<tr>
<td>MD5</td>
<td>128</td>
<td>128</td>
<td>512</td>
<td>64</td>
<td>32</td>
<td>Yes</td>
</tr>
<tr>
<td>PANAMA</td>
<td>256</td>
<td>8736</td>
<td>256</td>
<td>No</td>
<td>32</td>
<td>Yes</td>
</tr>
<tr>
<td>RadioGatn</td>
<td>Arbitrarily long</td>
<td>58 words</td>
<td>3 words</td>
<td>No</td>
<td>1-64</td>
<td>No</td>
</tr>
<tr>
<td>RIPEMD</td>
<td>128</td>
<td>128</td>
<td>512</td>
<td>64</td>
<td>32</td>
<td>Yes</td>
</tr>
<tr>
<td>RIPEMD</td>
<td>128/256</td>
<td>128/256</td>
<td>512</td>
<td>64</td>
<td>32</td>
<td>No</td>
</tr>
<tr>
<td>RIPEMD</td>
<td>160/320</td>
<td>160/320</td>
<td>512</td>
<td>64</td>
<td>32</td>
<td>No</td>
</tr>
<tr>
<td>SHA-0</td>
<td>160</td>
<td>160</td>
<td>512</td>
<td>64</td>
<td>32</td>
<td>Yes</td>
</tr>
<tr>
<td>SHA-1</td>
<td>160</td>
<td>160</td>
<td>512</td>
<td>64</td>
<td>32</td>
<td>With flaws</td>
</tr>
<tr>
<td>SHA-256/224</td>
<td>256/224</td>
<td>256</td>
<td>512</td>
<td>64</td>
<td>32</td>
<td>No</td>
</tr>
<tr>
<td>SHA-512/384</td>
<td>512/384</td>
<td>512</td>
<td>1024</td>
<td>128</td>
<td>64</td>
<td>No</td>
</tr>
<tr>
<td>Tiger(2)</td>
<td>192/160/128</td>
<td>192</td>
<td>512</td>
<td>64</td>
<td>64</td>
<td>No</td>
</tr>
<tr>
<td>WHIRLPOOL</td>
<td>512</td>
<td>512</td>
<td>512</td>
<td>256</td>
<td>8</td>
<td>No</td>
</tr>
</tbody>
</table>
SHA-3 Zoo

64 Submissions, 54 selected,

1. * BLAKE by Jean-Philippe Aumasson
2. Blue Midnight Wish by Svein Johan Knapskog
3. CubeHash by Daniel J. Bernstein preimage
4. ECHO by Henri Gilbert
5. Fugue by Charanjit S. Jutla
7. Hamsi by Özgül Küçü
8. * JH by Hongjun Wu preimage
9. * Keccak by The Keccak Team
10. Luffa by Dai Watanabe
11. Shabal by Jean-François Misarsky
12. SHA\textit{v}ite-3 by Orr Dunkelman
13. SIMD by Gaëtan Leurent
14. * Skein by Bruce Schneier
Birthday Paradox : Hash Function

Let an Hash function $H : D \rightarrow 2^k$

Naïve Collision
Birthday Paradox: Hash Function

Let an hash function $H : D \rightarrow 2^k$

Naïve Collision

With $2^k + 1$ try there is a collision

Table Collision
Birthday Paradox : Hash Function

Let an Hash function $H : D \rightarrow 2^k$

Naïve Collision

With $2^k + 1$ try there is a collision

Table Collision

- Try 1 : 0
Birthday Paradox : Hash Function

Let an Hash function \( H : D \rightarrow 2^k \)

Naïve Collision
With \( 2^k + 1 \) try there is a collision

Table Collision

- Try 1 : 0
- Try 2 : \( 1/2^k \)
Birthday Paradox: Hash Function

Let an Hash function $H : D \rightarrow 2^k$

Naïve Collision

With $2^k + 1$ try there is a collision

Table Collision

- Try 1: 0
- Try 2: $1/2^k$
- Try 3: $2/2^k$
Birthday Paradox : Hash Function

Let an Hash function $H : D \rightarrow 2^k$

Naïve Collision

With $2^k + 1$ try there is a collision

Table Collision

- Try 1 : 0
- Try 2 : $1/2^k$
- Try 3 : $2/2^k$
- ...
- Try $q : (q - 1)/2^k$
Birthday Paradox: Hash Function

Let an Hash function $H : D \rightarrow 2^k$

Naïve Collision

With $2^k + 1$ try there is a collision

Table Collision

- Try 1: 0
- Try 2: $1/2^k$
- Try 3: $2/2^k$
- ...
- Try $q$: $(q - 1)/2^k$

$$P(\text{collision}) = \sum_{i=1}^{i=q} i/2^k = q(q - 1)/2^{k+1}$$
Outline

Presentation

Motivations

Probabilities
  Mathematics Recalls
  Birthday Paradox
  Negligible Functions

Conclusion
Negligible functions

We call a function $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ negligible if for every positive polynomial $p$ there exists an $N$ such that for all $n > N$

$$\mu(n) < \frac{1}{p(n)}$$

Properties

Let $f$ and $g$ be two negligible functions, then

1. $f \cdot g$ is negligible.
2. For any $k > 0$, $f^k$ is negligible.
3. For any $\lambda, \mu$ in $\mathbb{R}$, $\lambda f + \mu g$ is negligible.

Exercise: Proofs
Negligible Functions

Exercise: Prove or disprove:

- The function $f(n) := \left(\frac{1}{2}\right)^n$ is negligible.
- The function $f(n) := 2^{-\sqrt{n}}$ is negligible.
- The function $f(n) := n^{-\log n}$ is negligible.
Noticeable Functions

Instead of ”there exists an $N$ such that for all $n > N$ ” we will in the following often say ”for all sufficiently large $n$”. We call a function $\nu : \mathbb{N} \rightarrow \mathbb{R}$ noticeable if there exists a positive polynomial $p$ such that for all sufficiently large $n$, we have:

$$\nu(n) > \frac{1}{p(n)}$$

Note: A function can be neither noticeable nor negligible.
Exercises

Prove or disprove the following statements:

1. If both \( f, g \geq 0 \) are noticeable, then \( f - g \) and \( f + g \) are noticeable.

2. If both \( f, g \geq 0 \) are not noticeable, then \( f - g \) is not noticeable.

3. If both \( f, g \geq 0 \) are not noticeable, then \( f + g \) is not noticeable.

4. If \( f \geq 0 \) is noticeable, and \( g \geq 0 \) is negligible, then \( f \cdot g \) is negligible.

5. If both \( f, g > 0 \) are negligible, then \( f/g \) is noticeable.
Outline

Presentation

Motivations

Probabilities
  Mathematics Recalls
  Birthday Paradox
  Negligible Functions

Conclusion
Today

1. Motivation
2. Probabilities (Random Variables)
3. Birthday Paradox
4. Negligeable Functions
Next Time

1. Indistinguishability
Thank you for your attention.

Questions?