TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Security and Cryptography 1

Stefan Köpsell, Thorsten Strufe

Module 3: A little reminder on discrete probability

Disclaimer: Thanks to Günter Schäfer, large parts actually taken from Dan Boneh

Dresden, WS 17/18

Reprise from Module 1

You have been introduced to some ***typical actors***

You understand what ***threats*** are … and what this means

You can tell ***security goals*** (*CIA!*) from ***security services***

You know ***adversary models*** and which aspects they define

Reprise from Module 2

You've learned the tuple (M,C,K,E,D)

You can tell the difference of

- Cryptology
- Cryptography
- Cryptanalysis

You know basic cryptanalysis (statistics/combinatorics)

You know transposition and substitution

You have learned the shift cipher

… Mono- and Polyalphabetic substitution ciphers

… Product ciphers

You know CT only attacks

And you have heard of the legends of Enigma and Alan Turing…

Module Outline

A few words on space and time

Probability distributions

Random variables

Independence

Randomized algorithms

Some characteristics of XOR

A few words on space and time

Recall shift cipher (Caesar)

- How many combinations of possible keys?

  2^5

- random guessing, how long do you need on average?

  2^4

Recall random permutation and Vigenère

- How large were the key spaces? 2^{88} 2^{122}
- How many random trials? 2^{87} 2^{121}

How large is large? (Some context)

Reference Numbers Comparing Relative Magnitudes			
Reference		***Magnitude***	
Seconds in a year		$\approx 3 * 10^{7}$	
Seconds since creation of solar system		$\approx 2 * 10^{17}$	$\approx 4.6 * 10^{9}$ y
Clock cycles per year (50 MHz computer)		$\approx 1.6 * 10^{15}$	
Instructions per year (i7 @ 3.0 GHz)	$\approx 2^{63}$	$\approx 7.15 * 10^{18}$	
Binary strings of length 64	2^{64}	$\approx 1.8 * 10^{19}$	
Binary strings of length 128	2^{128}	$\approx 3.4 * 10^{38}$	
Binary strings of length 256	2^{256}	$\approx 1.2 * 10^{77}$	
Number of 75-digit prime numbers		$\approx 5.2 * 10^{72}$	
Number of 80-digit prime numbers		$\approx 5.4 * 10^{77}$	
Electrons in the universe		$\approx 8.37 * 10^{77}$	

Attacking Cryptography: Brute Force Attack

Brute force attack, try all keys until intelligible plaintext found:

- Every crypto algorithm (save: OTP) can be attacked by brute force
- On average, half of all possible keys will have to be tried

Average Time Required for Exhaustive Key Search

Key Size [bit]	***Number of keys***	***Time required at 1 encryption / μs***	***Time required at 10^6 encryption / μs***
32	$2^{32} = 4.3 * 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 * 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 * 10^{38}$	2^{127} μs = $5.4 * 10^{24}$ years	$5.4 * 10^{18}$ years
(Vigenère 26 chars	26! = 4 $* 10^{26}$	2^{88} μs = $6.4*10^{12}$ years	$6.4*10^6$ years)

i7 could get to around 10^4 encryptions/μs
GPU can perform around $7x10^5$ hashes

Time since human/chimpanzee lines diverged:
$5×10^6$ years,
Homo sapiens: $5×10^4$ years

Recap: Discrete Probabilities

U: finite set (e.g. $U = \{0,1\}^n$)

Def: **Probability distribution** P over U is a function $P: U \longrightarrow \mathbb{R}^+$

more specifically $P(x) \in [0,1]$

such that $\sum P(x) = 1$

Examples:

1. Uniform distribution: for all $x \in U$: $P(x) = 1/|U|$
2. Point distribution at x_0: $P(x_0) = 1$, $\forall x \neq x_0$: $P(x) = 0$

Examples

Fair coin:

U = {H,T}, P(H)=P(T) = ½

Dice:

U= {1,…,6}, P(x) = 1/6, $1 \leq x \leq 6$

Two dice (combined):

U= {1,..,6}^{2} ={(x1,x2): $1 \leq x_1, x_2 \leq 6$}

P(x_1, x_2) = 1/36 for all x_1, x_2

Uniform distributions for all of the above

Two dice (sum):

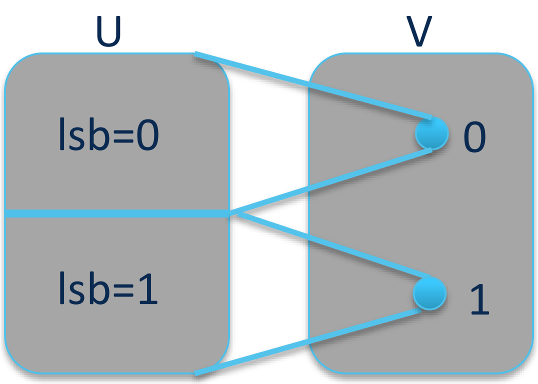
U= {2,3,…,12}

P(2)= 1/36, P(3)=2/36,…,P(12)=1/36

Random Variables

Def: a random variable X is a function $X:U \longrightarrow V$

Example: $X: \{0,1\}^n \longrightarrow \{0,1\}$; $X(y) = \text{lsb}(y) \in \{0,1\}$



For the uniform distribution on U:

$\Pr[\, X=0 \,] = 1/2$, $\Pr[\, X=1 \,] = 1/2$

More generally:

rand. var. X induces a distribution on V: $\Pr[\, X=v \,] := \Pr\left[\, X^{-1}(v) \,\right]$

The uniform random variable

Let U be some set, e.g. $U = \{0,1\}^n$

We write $r \xleftarrow{R} U$ to denote a **uniform random variable** over U

for all $a \in U$: $\Pr\left[\, r = a \,\right] = 1/|U|$

Let r be a uniform random variable on $\{0,1\}^2$

Define the random variable $X = r_1 + r_2$

Then $\Pr[X=2] = \boxed{}$

The uniform random variable

Let U be some set, e.g. $U = \{0,1\}^n$

We write $r \xleftarrow{R} U$ to denote a **uniform random variable** over U

for all $a \in U$: $\Pr\big[\, r = a \,\big] = 1/|U|$

Let r be a uniform random variable on $\{0,1\}^2$

Define the random variable $X = r_1 + r_2$

Then $\Pr[X=2] = ¼$

Events

For a set $A \subseteq U$: $\Pr[A] = \sum_{x \in A} P(x) \in [0,1]$

note: $\Pr[U]=1$

The set A is called an **event**

Example: $U = \{0,1\}^8$

$A = \{$ all x in U such that $lsb_2(x)=11$ $\} \subseteq U$

for the uniform distribution on $\{0,1\}^8$: Pr[A]

What about $U = \{0,1\}^n$ (with n>2)?

Events

For a set $A \subseteq U$: $\Pr[A] = \sum_{x \in A} P(x) \in [0,1]$

note: $\Pr[U]=1$

The set A is called an **event**

Example: $U = \{0,1\}^8$

$A = \{$ all x in U such that $\mathrm{lsb}_2(x)=11$ $\} \subseteq U$

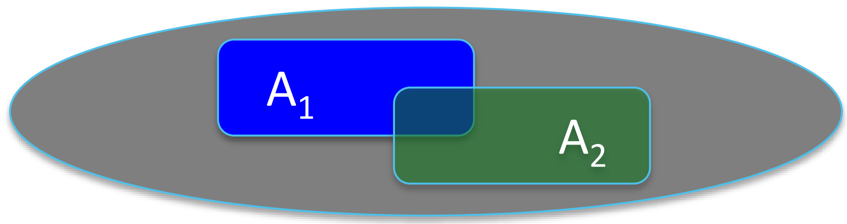
for the uniform distribution on $\{0,1\}^8$: $\Pr[A] = 1/4$

What about $U = \{0,1\}^n$ (with $n>2$)?

Boole`s Inequality / The Union Bound

For events A_1 and A_2

$$\Pr[\, A_1 \cup A_2 \,] \leq \Pr[A_1] + \Pr[A_2]$$



$$A_1 \cap A_2 = \emptyset \rightarrow \Pr[A_1 \cup A_2] = \Pr[A_1] + \Pr[A_2]$$

Example:

$$A_1 = \{ \text{ all } x \text{ in } \{0,1\}^n \text{ s.t } \mathrm{lsb}_2(x)=11 \ \} ;$$

$$A_2 = \{ \text{ all } x \text{ in } \{0,1\}^n \text{ s.t. } \mathrm{msb}_2(x)=11 \ \}$$

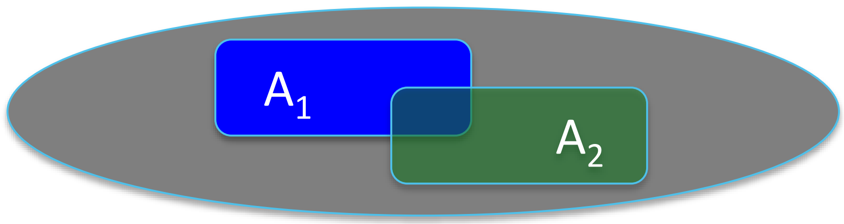
$$\Pr[\, \mathrm{lsb}_2(x)=11 \text{ or } \mathrm{msb}_2(x)=11 \,] = \Pr[A_1 \cup A_2] \leq$$

When is it less than 1/2?

Boole`s Inequality / The Union Bound

For events A_1 and A_2

$$\Pr\left[A_1 \cup A_2 \right] \leq \Pr[A_1] + \Pr[A_2]$$



$$A_1 \cap A_2 = \emptyset \rightarrow \Pr[A_1 \cup A_2] = \Pr[A_1] + \Pr[A_2]$$

Example:

$$A_1 = \{ \text{ all } x \text{ in } \{0,1\}^n \text{ s.t } lsb_2(x)=11 \ \} ;$$
$$A_2 = \{ \text{ all } x \text{ in } \{0,1\}^n \text{ s.t. } msb_2(x)=11 \ \}$$

$$\Pr\left[lsb_2(x)=11 \text{ or } msb_2(x)=11 \right] = \Pr\left[A_1 \cup A_2\right] \leq \tfrac{1}{4}+\tfrac{1}{4} = \tfrac{1}{2}$$

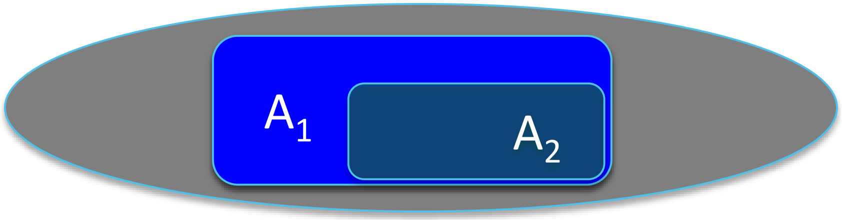
When is it less than 1/2?

Conditional Probabilities

Suppose event $A \subseteq U$.

The *induced* probability P_A is defined as:

$$P_A(x) = \frac{P(x)}{P(A)} \text{ for x} \in \text{A}$$



For two events, $A_1, A_2 \subseteq U$ we say that $P_{A_1}(A_2)$, or $P(A_2|A_1)$ is

$$P(A_2|A_1) = P_{A_1}(A_1 \cap A_2) = \frac{P(A_1 \cap A_2)}{P(A_1)}$$

Another Example

For events A_1 and A_2:

$$A_1 = \{x \; in \; \{0,1\}^3 : msb(x) = 1\}$$
$$A_2 = \{x \; in \; \{0,1\}^3 : x < 110\}$$

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

$$P(A_1 \cap A_2) = \{x \; in \; \{0,1\}^3 : msb(x) = 1, x < 110\}$$

What if:
$A_1 = \{x \; in \; \{0,1\}^3 : lsb(x) = 1\}$?

$$P(A_1) =$$

$$P(A_1 \cap A_2) =$$

$$P(A_2 | A_1) =$$

...we call A_1 and A_2 ***independent*** if $P(A_2|A_1) = P(A_2)$

Another Example

For events A_1 and A_2:

$$A_1 = \{x \; in \; \{0,1\}^3 : msb(x) = 1\}$$
$$A_2 = \{x \; in \; \{0,1\}^3 : x < 110\}$$

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

$$P(A_1 \cap A_2) = \{x \; in \; \{0,1\}^3 : msb(x) = 1, x < 110\}$$

What if:
$A_1 = \{x \; in \; \{0,1\}^3 : lsb(x) = 1\}$?

$$P(A_1) = 1/2$$
$$P(A_1 \cap A_2) = 2/8 = 1/4$$

$$P(A_2|A_1) = \frac{1/4}{1/2} = 1/2$$

…we call A_1 and A_2 ***independent*** if $P(A_2|A_1) = P(A_2)$

Independence

Definition:

Events A_1 and A_2 are ***independent***, if Pr[A_1 and A_2]=Pr[A_1] x Pr[A_2]

Random variables X,Y, both taking values in V are ***independent*** if

$$\forall a,b \in V: \quad \Pr[X=a \text{ and } Y=b] = \Pr[X=a] \times \Pr[Y=b]$$

Example:

$$U = \{0,1\}^2 = \{00, 01, 10, 11\} \qquad \text{and} \qquad r \xleftarrow{R} U$$

Define random variables X and Y as: $X = \mathrm{lsb}(r)$, $Y = \mathrm{msb}(r)$

Pr[X=0 and Y=0] =

Independence

Definition:

Events A_1 and A_2 are ***independent***, if Pr[A_1 and A_2]=Pr[A_1] x Pr[A_2]

Random variables X,Y, both taking values in V are ***independent*** if

$$\forall a,b \in V: \quad \Pr[X=a \text{ and } Y=b] = \Pr[X=a] \times \Pr[Y=b]$$

Example:

$$U = \{0,1\}^2 = \{00, 01, 10, 11\} \quad \text{and} \quad r \xleftarrow{R} U$$

Define random variables X and Y as: $X = \mathrm{lsb}(r)$, $Y = \mathrm{msb}(r)$

$$\Pr[X=0 \text{ and } Y=0] = \Pr[r=00] = 1/4 = \Pr[X=0] \times \Pr[Y=0]$$

Randomized Algorithm

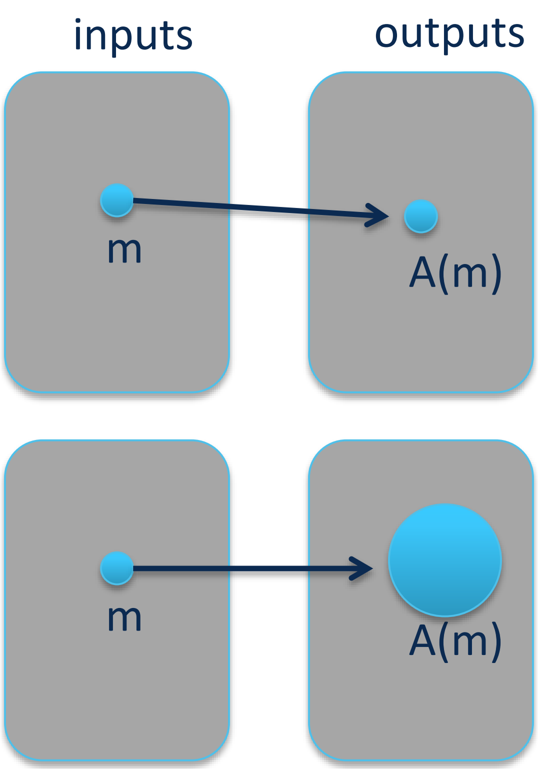
Deterministic algorithm: $y \longleftarrow A(m)$

Randomized algorithm

$y \longleftarrow A(m\,;r)$ where $r \overset{R}{\longleftarrow} \{0,1\}^n$

output is a random variable

$y \overset{R}{\longleftarrow} A(m)$



Example: $A(m\,;k) = E(k, m)$, $y \overset{R}{\longleftarrow} A(m)$

The cryptographer‘s workhorse: XOR

XOR of two strings in $\{0,1\}^n$ is their bitwise addition mod 2:

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

1	1	0	1	0	1	0	1	$\oplus$
1	0	1	1	1	0	1	1	
0	1	1	0					

Theorem:

Let Y be a random variable over $\{0,1\}^n$

Let X be an independent uniform variable on $\{0,1\}^n$

X	Pr
0	p_0
1	p_1

Y	Pr
0	1/2
1	1/2

Then $Z := Y \oplus X$ is uniform var. on $\{0,1\}^n$:

$\Pr[Z=0]$

$= \Pr[(x,y)=(0,0) \text{ or } (x,y)=(1,1)]$

$= \Pr[(x,y)=(0,0)] + \Pr[(x,y)=(1,1)] =$

x	y	Pr
0	0	$p_0/2$
0	1	$p_0/2$
1	0	$p_1/2$
1	1	$p_1/2$

The cryptographer's workhorse: XOR

XOR of two strings in $\{0,1\}^n$ is their bitwise addition mod 2:

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

	1	1	0	1	0	1	0	1
$\oplus$	1	0	1	1	1	0	1	1
	0	1	1	0	1	1	1	0

Theorem:

Let Y be a random variable over $\{0,1\}^n$

Let X be an independent uniform variable on $\{0,1\}^n$

Then $Z := Y \oplus X$ is uniform var. on $\{0,1\}^n$:

X	Pr
0	p_0
1	p_1

Y	Pr
0	1/2
1	1/2

Pr[Z=0]

= Pr[(x,y)=(0,0) or (x,y)=(1,1)]

$= \Pr[(x,y)=(0,0)] + \Pr[(x,y)=(1,1)] = p_0/2 + p_1/2 = 1/2$

x	y	Pr
0	0	$p_0/2$
0	1	$p_0/2$
1	0	$p_1/2$
1	1	$p_1/2$

Summary

You now recall:

probability distributions, random variables, randomized algorithms, independence – and the beauty of XOR! ;-)