CS4236 Cryptography Theory and Practice Topic 2 - Perfect secrecy

Hugh Anderson

National University of Singapore
School of Computing

August, 2022

One time pad...

Outline

1. **JIT mathematics**
   - Probability (for today)
   - Modulo arithmetic (for today), and fields (for later)

2. **Perfect secrecy**
   - The one time pad
   - Perfect secrecy more formally
   - The modern approach

Probability - variables and events

Definitions: random variables, and events

Random Variable X: A variable where each value is associated with a certain probability (non-negative real numbers that sum to 1).
Events: The outcome of a random process.

Example with red and blue dice

X: the value of a randomly thrown (red) die
Y: the value of another (blue) die.

Here X, Y are random variables.

The outcome X=1 is an event. The events X=1, X=2, X=3, . . . , X=6 are mutually exclusive.
If the two dice are thrown “independently” without influencing each other, then X, Y are independent random variables. The events X=1, Y=1 are independent.

Probability - events

Definitions: independent and mutually exclusive

Independent: (the two processes don't interact with each other, and thus don't influence each other)

If E_1, E_2 are independent events, then

$$\Pr[E_1 \wedge E_2] = \Pr[E_1, E_2] = \Pr[E_1] \times \Pr[E_2]$$

If X, Y are independent random variables then for all x,y

$$\Pr[X = x \wedge Y = y] = \Pr[X = x] \times \Pr[Y = y]$$

Mutually exclusive: (you can't do both at the same time).

If E_1, E_2 are two mutually exclusive events, then

$$\Pr[E_1 \vee E_2] = \Pr[E_1] + \Pr[E_2]$$

and also $\Pr[E_1 \wedge E_2] = 0$

Probability - types

Definitions: joint and conditional probability

Joint Probability: $\Pr[X = x \wedge Y = y]$ (often abbreviated to $\Pr[x, y]$)

Conditional Probability: $\Pr[X = x | Y = y] = \Pr[x|y] \stackrel{def}{=} \frac{\Pr[x,y]}{\Pr[y]}$ (if $\Pr[y] \neq 0$)

For any value y, we can define a random variable A, where

$$\Pr[A = x] = \Pr[X = x | Y = y]$$

For convenience we write $X|Y = y$ as this random variable (Not $X|Y$).

A useful formula: $\Pr[x, y] = \Pr[x|y] \times \Pr[y]$

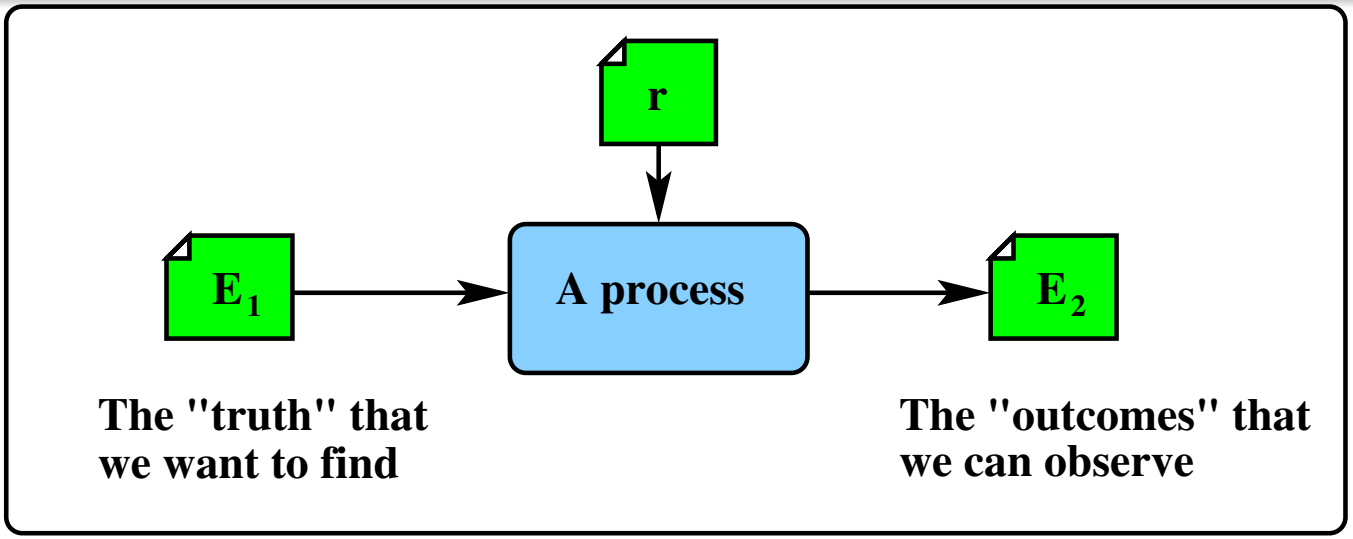
$\Pr[X = x, Y = y]$	$X = 1$	$X = 2$	$X = 3$
$Y = 1$	0.4	0.05	0.05
$Y = 2$	0	0.1	0.4

The events X=1,Y=1 are not independent. $(0.5 * 0.4 = 0.2) \neq 0.4$

$\Pr[Y = 1] = \ldots = 0.5$
$\Pr[X = 1 | Y = 1] = \ldots = 0.8$
$\Pr[X = 3 | Y = 1] = \ldots = 0.1$

$\Pr[X = 1] = \ldots = 0.4$
$\Pr[X = 2 | Y = 1] = \ldots = 0.1$

Baye's theorem



The theorem:

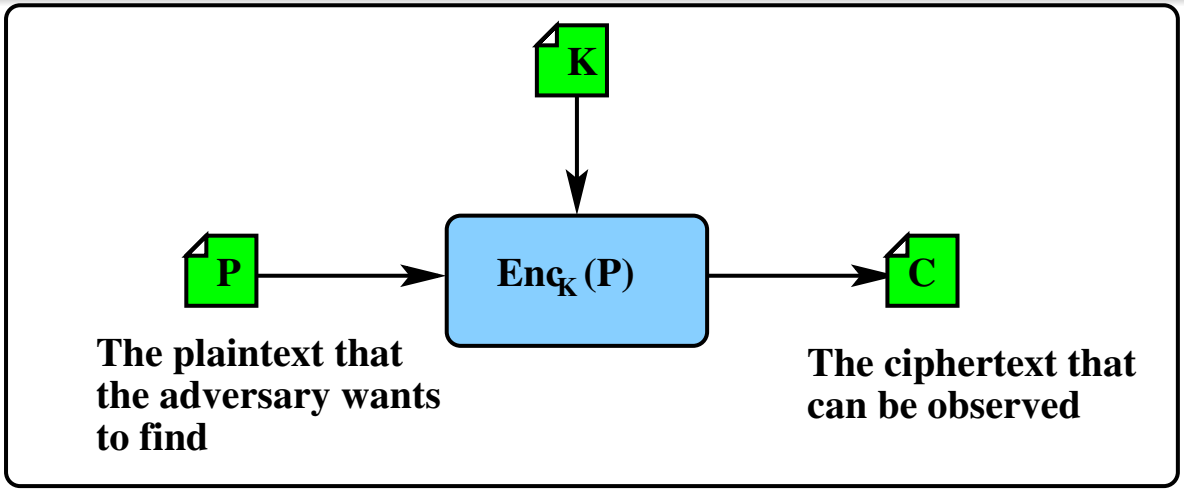
If $\Pr[E_2] \neq 0$, then

$$\Pr[E_1|E_2] = \frac{\Pr[E_2|E_1] \times \Pr[E_1]}{\Pr[E_2]}$$

An interpretation

Note that the term on the left $\Pr[E_1|E_2]$ is the *posterior* probability - what we know after observing the outcome. Note also that $\Pr[E_1]$ is the *prior* probability - what we know without observing the outcome.
Bayes theorem relates *a priori* and *a posteriori* probabilities.

Baye's theorem $\Pr[E_1|E_2] = \frac{\Pr[E_2|E_1] \times \Pr[E_1]}{\Pr[E_2]}$



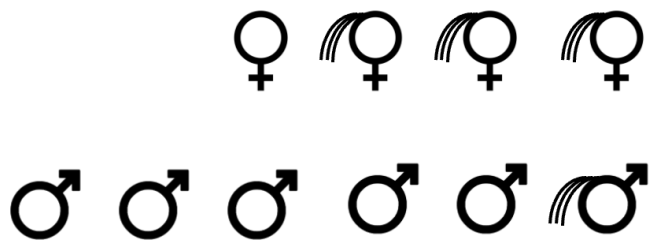
Relevance to crypto

In the context of cryptography, one can imagine throwing two independent dice. One of them is the message P, and the other the key K. Next, a ciphertext is computed from the plaintext and key. Since the key and plaintext are randomly chosen, the ciphertext C is thus also random.

Now, an adversary has observed the ciphertext and thus knows that C=3. The adversary wants to know what are the chances that the plaintext is 5, given that the ciphertext is 3, that is, the probability

$$\Pr[P = 5|C = 3]$$

Practice exercise: scenario 1



Pr[X,Y]	Long	Short
Female	0.3	0.1
Male	0.1	0.5

Example 1

Assume that in the corridor, there were 4 women, 3 with long hair, and 6 men, 1 with long hair.
The Lecturer asked a random person from the corridor to join in the class and he/she sat at the back of the classroom. The lecturer asked each student without looking to guess the mystery person's sex. If a student was correct, they would win $1, otherwise would lose $1.50

1. What would be your guess? What is your expected gain?
2. Suppose you cheated and peeped. You saw that the mystery person had long hair. What would be your guess? What is your expected gain?

Let X be the random variable on the sex and Y the hair length.

How to work out gain...

Expected return/gain

The expected return is calculated by using the following formula:

$$E[R] = \sum_{i=1}^{n} R_i P_i$$

where

- R_i is the return in a particular scenario i;
- P_i is the probability for the return R_i;
- and n, the number of scenarios.

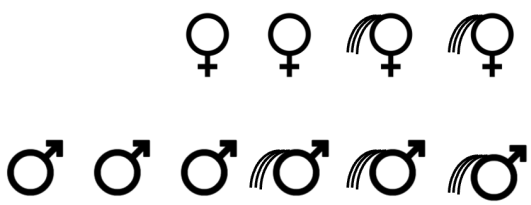
Example (1) from scenario 1...

Assuming that the student makes a guess and bets on *male*, then there are two scenarios - either $X = m$ (win), or $X = f$ (lose). So

$$\begin{aligned} E[R] &= 1.00 \times \Pr[X = m] + (-1.50) \times \Pr[X = f] \\ &= 0.6 - 0.6 = 0 \end{aligned}$$

So for each student *male* guess, the expected return is \$0.00. What if the student bet on a *female*?

Practice exercise: scenario 2



Example 2

Repeat scenario 1 for the situation when 2 women have long hair, and 3 men have long hair. Does knowing length help guess sex?

Hints

1. The joint probability can be determined by counting the number of persons in each combination. In scenario 1, $\Pr[X = f, Y = \ell] = \frac{3}{10} = 0.3$.
2. Want to maximize the expected gain. Compare $\Pr[X = f] = 0.4$ with $\Pr[X = m] = 0.6$
3. Compare $\Pr[X = f | Y = \ell]$ with $\Pr[X = m | Y = \ell]$

Practice exercise: crypto

The context:

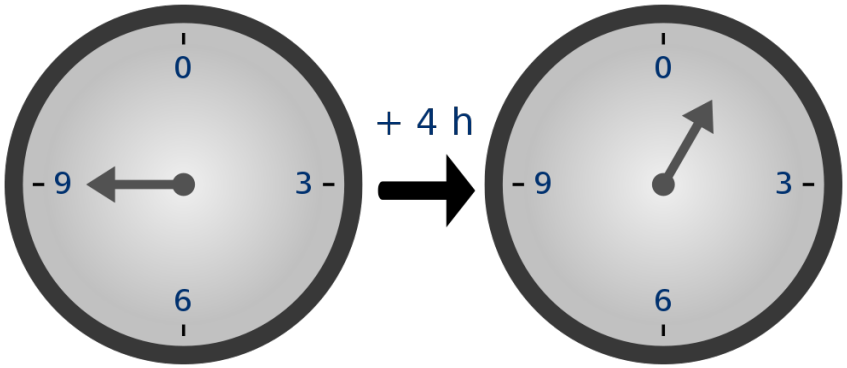
In most cryptography schemes that involve arithmetic, the operation (addition, multiplication) is "modulo" and thus the domain is $\mathbb{Z}_n$.
Consider a shift cipher that operates in the domain $\mathbb{Z}$. (i.e. no modulo), where the key and the message are integers uniformly and randomly chosen from $\{0, 1, 2, 3, 4, 5\}$.
The encryption is $\mathrm{Enc}_k(x) = x + k$ (note, no modulo). Why is this not secure?

Examples

Find the following:

1. $\Pr[C = 0], \Pr[C = 1], \ldots$
2. $\Pr[X = 1, K = 2 | C = 5]$, $\Pr[X = 1 | C = 5, K = 2]$.
3. $\Pr[K = 3 | X = 2]$.
4. $\Pr[X = 0 | C = 5]$, $\Pr[X = 1 | C = 5]$, ... i.e. the distribution $X | C = 5$.
5. $\Pr[X = 0 | C = 1]$, $\Pr[X = 1 | C = 1]$,....

Modular (clock) arithmetic: $+, *$ in $\mathbb{Z}_7$



+,* in $\mathbb{Z}_7$

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	**1**	**2**	**3**	**4**	**5**	**6**
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Steps towards finite fields

Closed algebraic systems: a group is

- a set of *group elements* with
- a *binary operation* $\bullet$

If one denotes the group operation by $\bullet$, then the above says that for any group elements a and b, $a \bullet b$ is defined and is also a group element (i.e. it is closed)

For all group elements a,b,c, GROUPS..

- are *associative*, meaning that $a \bullet (b \bullet c) = (a \bullet b) \bullet c$
- have an *identity* e satisfying $a \bullet e = e \bullet a = a$ for any a.
- have an *inverse* a^{-1} satisfying $a \bullet a^{-1} = a^{-1} \bullet a = e$.

and if $a \bullet b = b \bullet a$ then the group is *commutative* or *abelian*. Otherwise it is *non-commutative*. Notice that even in a non-commutative group, $a \bullet b = b \bullet a$ might sometimes be true for example if a or b is the identity. A group with only finitely many elements is called *finite*; otherwise it is *infinite*.

Examples

Infinite groups: (Integers,+), and (positive rationals,*)

1. The *integers* (all whole numbers, including 0 and negative numbers) form an infinite commutative group using addition. The identity is 0 and the inverse of a is $-a$.
2. The *positive rationals* (all positive fractions, including all positive integers) form a group if ordinary multiplication is the operation. The identity is 1 and the inverse of r is $1/r = r^{-1}$.

Finite group: (Integers (mod N),+ (mod N))

The *integers mod n* form a group for any integer $n > 0$. This group is often denoted $\mathbb{Z}_n$. Here the elements are $0, 1, 2, \ldots, n-1$ and the operation is addition followed by remainder on division by n. The identity is 0 and the inverse of a is $n - a$ (except for 0 which is its own inverse).

Fields (for later)

A field has two operations traditionally called + and *

> $+$, *with elements of the field forming a commutative group. Identity is* 0 *and inverse of* a *is* $-a$.
> $*$, *with elements of the field except* 0 *forming another commutative group, identity denoted by* 1 *and inverse of* a *denoted by* a^{-1}.

There is also the *distributive identity*, linking $+$ and $*$:

$$a * (b + c) = (a * b) + (a * c)$$

If c is not zero and $a * c = b * c$, then $a = b$.

Examples of fields

Infinite fields: rationals, reals and complex numbers

The *rational numbers* (fractions) $\mathbb{Q}$, or the *real numbers* $\mathbb{R}$, or the *complex numbers* $\mathbb{C}$, using ordinary addition and multiplication (extended in the last case to the complex numbers).

Finite field: Integers modulo a prime

The *integers mod p*, denoted $\mathbb{Z}_p$, where p is a prime number (2, 3, 5, 7, 11, 13, 17, 19, 23, 29, . . .).

- A group using $+$.
- Elements without 0 form a group under $*$.
- The identity is clearly 1, but
- the inverse of a non-zero element *a* is not obvious.

Modular arithmetic: $+, *$ inverses in $\mathbb{Z}_7$

Properties of elements for a field ($\mathbb{Z}_7$,+,*)

a	$-a$	a^{-1}
0	0	-
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

- Additive inverse:
  $a + (-a) \bmod p = 0$
- Multiplicative inverse:
  $(a * a^{-1}) \bmod p = 1$.
- Reducibility:
  - $(a + b) \bmod p =$
    $(a \bmod p + b \bmod p) \bmod p$
  - $(a * b) \bmod p =$
    $(a \bmod p * b \bmod p) \bmod p$

Modular arithmetic: $+, *$ in $\mathbb{Z}_8$

Lets look at modular arithmetic in $\mathbb{Z}_8$

$+$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$*$	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	2
7	7	6	5	4	3	2	1

Modular arithmetic: $+, *$ inverses in $\mathbb{Z}_8$?

... and the inverses go bad ...

a	$-a$	a^{-1}
0	0	-
1	7	1
2	6	-
3	5	3
4	4	-
5	3	5
6	2	-
7	1	7

By changing the definitions for $+$ and $*$ we will be able to have an algebraic number field in $\mathbb{Z}_8$.

A field of size 8 ...

The tables for arithmetic in $\mathrm{GF}(2^3)$

$+$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

$*$	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	1	2	3	4	5	6	7
2	2	4	6	3	1	7	5
3	3	6	5	7	4	1	2
4	4	3	7	6	2	5	1
5	5	1	4	2	7	3	6
6	6	7	1	5	3	2	4
7	7	5	2	1	6	4	3

How to compute the table values?

Obviously not multiplication (modulo 8), but the techniques are analogous to that... remainder after division by an irreducible polynomial.
Handout has details.

Polynomial operations - addition

Polynomials are expressions like $3x^5 + x^2 + x + 1$

More generally, a (univariate) polynomial of degree n is $\sum_{i=0}^{n} a_i x^i$. A particular set of such polynomials is the set where the coefficients a_i belong to $\mathbb{Z}_p$. In the case where $p = 2$, then the coefficients are either 0 or 1.
In this restricted case, polynomial addition becomes the same as the **`xor`** function over the coefficients. Consider the addition of 3 and 6:

	$3 = 011$	$x + 1$
$\oplus$	$6 = 110$	$x^2 + x$
	$5 = 101$	$x^2 + 1$

Polynomial multiplication

Multiplication follows a similar pattern

But when the multiplication results in too large a polynomial, then we reduce it, by dividing it by an irreducible polynomial of degree n, and take the residue. In the case of $n = 3$, a polynomial like $x^3 + x + 1 = 1011$ is irreducible. An example, 7×7:

	$7 =$	111						x^2	$+$	x	$+$	1
$*$	$7 =$	111	$*$					x^2	$+$	x	$+$	1
		111						x^2	$+$	x	$+$	1
	$\oplus$	1110				x^3	$+$	x^2	$+$	x		
	$\oplus$	11100		x^4	$+$	x^3	$+$	x^2				
		10101		x^4			$+$	x^2			$+$	1

Polynomial multiplication

Dividing by an irreducible polynomial

The result polynomial is too large, so we reduce it, using polynomial long division, with the result being the remainder:

$$
\begin{array}{rr|l}
 & 10 & \\
\cline{2-2}
1011 & 10101 & x^3 + x + 1 \;\big|\; x^4 + x^2 + 1 \\
 & \underline{1011} & \quad\; x^4 + x^2 + x \\
\cline{2-2}
 & 11 & \quad\; x + 1
\end{array}
$$

Finally, we have that in $\mathrm{GF}(2^3)$, $7 * 7 = 3$.

Mutiplicative groups for field of size 8 ...

There are two irreducible polynomials in $\mathrm{GF}(2^3)$

$p(x) = x^3 + x + 1 = 1011$

$*$	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	1	2	3	4	5	6	7
2	2	4	6	3	1	7	5
3	3	6	5	7	4	1	2
4	4	3	7	6	2	5	1
5	5	1	4	2	7	3	6
6	6	7	1	5	3	2	4
7	7	5	2	1	6	4	3

$p(x) = x^3 + x^2 + 1 = 1101$

$*$	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	1	2	3	4	5	6	7
2	2	4	6	5	7	1	3
3	3	6	5	1	2	7	4
4	4	5	1	7	3	2	6
5	5	7	2	3	6	4	1
6	6	1	7	2	4	3	5
7	7	3	4	6	1	5	2

They look different, but....

... it is possible to see they are the same using renaming of the values. Finite fields of the same size are unique modulo renaming.

Relevance of fields/groups

Finite fields and groups are important in crypto

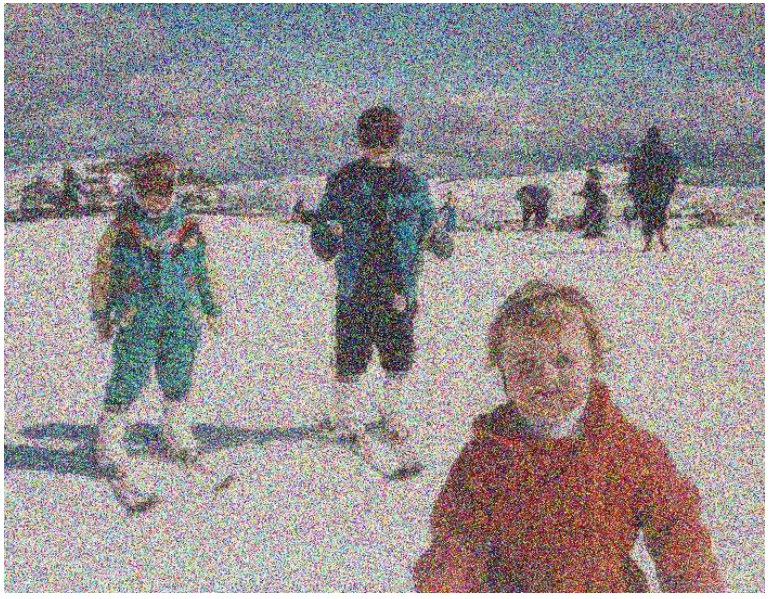
Finite fields, in particular, are important because the operations associated with them work as expected inside the field. We will not suddenly do an operation and discover that the result is somehow outside the field.

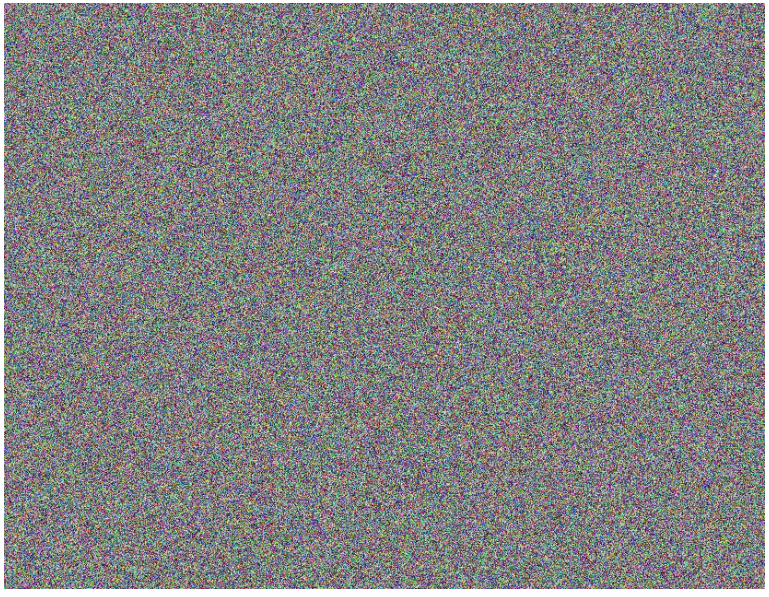
Each field has two operations (and their inverses) defined over them. In the example given over $\mathbb{Z}_7$, we see that the additive operation forms a nice (commutative) group over the elements 0 to 6, and that the multiplicative operation forms a nice (commutative) group over the elements 1 to 6. Note that the set $\{1, \ldots, 6\}$ is just the other set, less the additive identity (0): $\{1, \ldots, 6\} = \{0, \ldots, 6\} \backslash 0$.

An interesting property of fields is that fields of the same size are unique modulo renaming. What this means is that any field of size 7, no matter what the symbols used for it, and no matter how the operations are defined, would have a mapping from those symbols to numbers, and it would look EXACTLY like the field $\mathbb{Z}_7$, shown in class.

Fields are a more abstract notion than just “things defined over sets of numbers”. Later in the course we will see fields appearing in AES and ECC.

Random bit changes, 0%, 25%, 50% and 100%





50%, but not random: every second bit

One time pad/Vernam's cipher

An "unconditionally secure" scheme:

- One time pad provides perfect secrecy.
- The key is a sequence of random key letters, each letter used once only, and available at only the sender and receiver.

Binary and integer examples

Plaintext	0100101001	1,5,3,11,8
	$\oplus$	$+ \bmod 12$
Key	0011001101	3,9,0,7,4
	$=$	$=$
Ciphertext	0111100100	4,2,3,6,0

Note that there are no real differences between the binary XOR function and the addition modulo a number. XOR is just addition modulo 2.

A symmetric scheme construction: One time pad

Formal definition: $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$

$\mathrm{Gen}(1^n)$: The key is a random sequence of elements in $\mathbb{Z}_n$:
$K = k_1, k_2, k_3, \ldots$

$\mathrm{Enc}_k(X)$: The plaintext is a sequence of elements in $\mathbb{Z}_n$,

$$X = x_1, x_2, x_3, \ldots$$

The ciphertext is

this is the formal definiti

$$Y = \mathrm{Enc}_k(X) = (k_1 + x_1) \bmod n, (k_2 + x_2) \bmod n, \ldots$$

$\mathrm{Dec}_k(Y)$: To decrypt the ciphertext $Y = y_1, y_2, y_3, \ldots$, the plaintext is

$$X = \mathrm{Dec}_k(Y) = (y_1 - k_1) \bmod n, (y_2 - k_2) \bmod n, \ldots$$

Commentary

Correctness: Note that $x_i = ((x_i + k_i) \bmod n) – k_i) \bmod n$

When $n = 2$, then the key is a sequence of binary bits, and encryption (and decryption) is equivalent to *xor'ing* the key. If the length of the (random) bitstring is ℓ then the probability of $X = Y$ is $2^{-\ell}$.

One time pad - shock horror!

It is “perfectly” secret

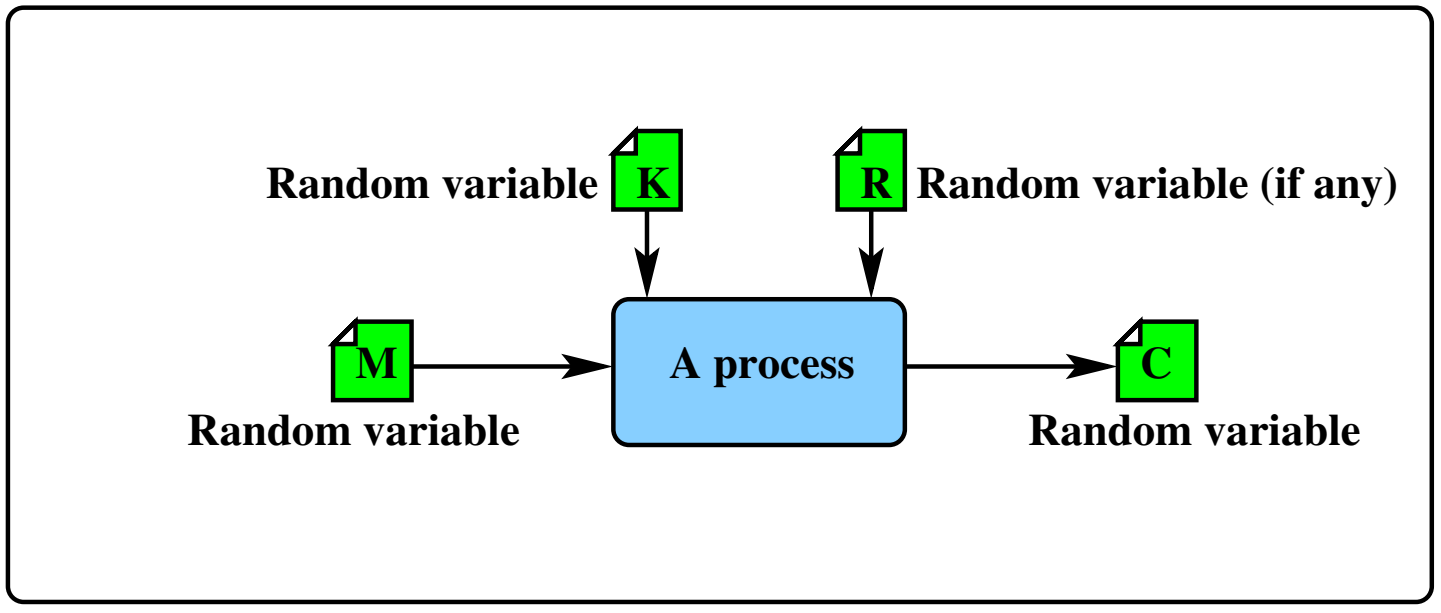
The one-time-pad is “guaranteed” to be unbreakable even if the adversary has arbitrary long computing time. It provides “perfect secrecy” (to be defined).
Why it is not practical in most scenarios? In which scenario is it useful?

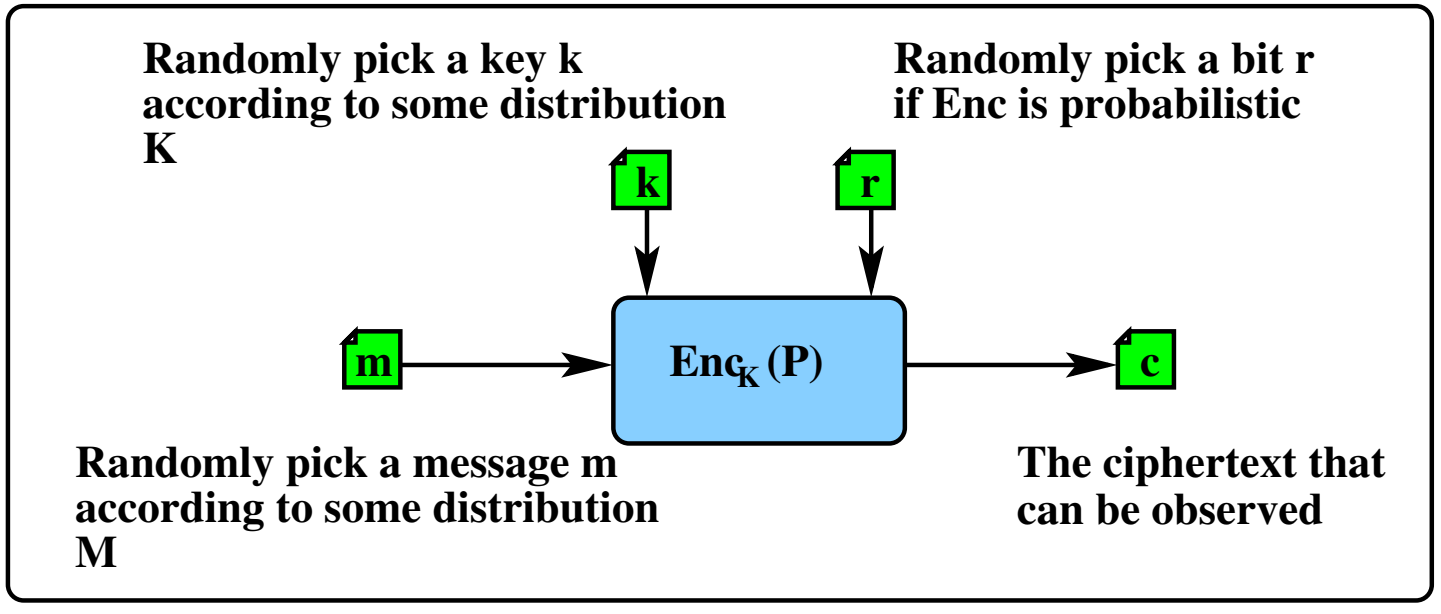
Examples

Soviet diplomatic telegrams were encrypted by a one-time pad, which is “unbreakable”. However, they reused some of the key. Due to this loophole, some messages were de-ciphered by the US’s Venona project.

It was also observed that the keys were probably typed using a typewriter, and thus not truly random. However, it is not clear whether this observation had been exploited in the Venona project.
`https://www.nsa.gov/Portals/70/documents/about/cryptologic-heritage/historical-figures-publications/publications/coldwar/venona_story.pdf`

Prior probability, posterior probability

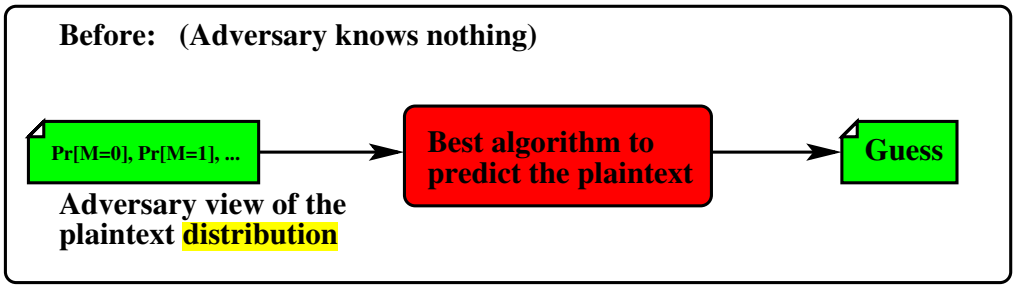




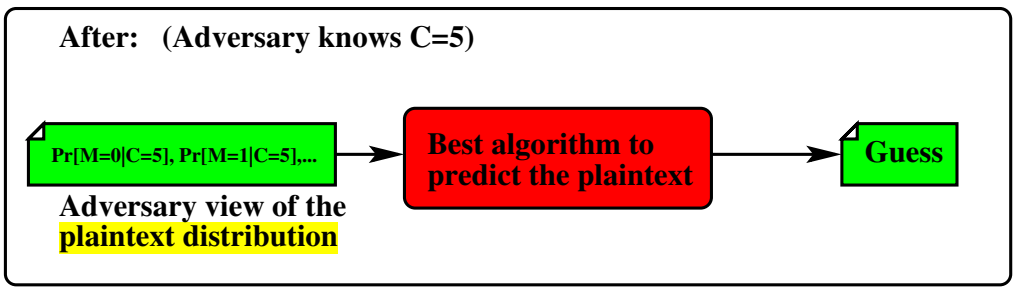
Prior probability, posterior probability

Relating to our encryption scheme:

Prior probability: Let M be distribution of plaintext. $\Pr[M = m]$ is the prior probability that the plaintext m occurred. It is the adversary's knowledge of the plaintext before seeing the ciphertext.



Posterior probability: Let m and c be a message and ciphertext respectively. $\Pr[M = m|C = c]$ is the posterior probability. It is the adversary's knowledge of the plaintext after seeing the particular ciphertext c.



Perfectly secret if knowing ciphertext is no help...

Definition 2.3

An encryption scheme $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is perfectly secure if, for any distribution M over its message space $\mathcal{M}$, for all $m \in \mathcal{M}$, $c \in \mathcal{C}$, then

$$\Pr[M = m | C = c] = \Pr[M = m]$$

where the probability includes choice of key and any randomness of Enc. Note also that $\Pr[C = c] > 0$. Loosely, knowing the ciphertext reveals nothing about the plaintext.

Definition 2.3(a)

An encryption scheme $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is (also) perfectly secure if, for all $m, m' \in \mathcal{M}$, $c \in \mathcal{C}$

$$\Pr[\mathrm{Enc}_k(m) = c] = \Pr[\mathrm{Enc}_k(m') = c]$$

where the probability includes choice of key and any randomness of Enc. Loosely, the distribution of the ciphertext is identical if you encrypt any messages (m or m').

“Proving” things...

How do we prove something? 3 ways...

If we wanted to prove that $p \Rightarrow q$ (p implies q, or if p then q), then we might use

- **Direct, or Constructive proof**: a straightforward combination or sequence of established facts (axioms), theorems/lemmas, and agreed inference rules.
- **Proof by contradiction** (Suppose Not!): We could use techniques like these:
  - Assume $p \Rightarrow \neg q$, and then derive a contradiction - for example $x \wedge \neg x$
  - Prove $\neg q \Rightarrow \neg p$ a direct proof of the contrapositive

Finally, we might use an **Inductive proof** - prove a basis case and an inductive step.

Sample proof of... Bayes theorem

Bayes theorem is a theorem, not a definition...

... so we can *prove* it. We want to *prove* that $\Pr[E_1|E_2] = \frac{\Pr[E_2|E_1]\times\Pr[E_1]}{\Pr[E_2]}$, so, starting with things we know...

$$
\begin{array}{lllll}
 & \Pr[E_1|E_2] & = & \frac{\Pr[E_1\wedge E_2]}{\Pr[E_2]} & (\text{Why?}) \\
\text{and} & \Pr[E_2|E_1] & = & \frac{\Pr[E_2\wedge E_1]}{\Pr[E_1]} & (\text{Why?}) \\
\text{so} & \Pr[E_1|E_2]\times\Pr[E_2] & = & \Pr[E_2|E_1]\times\Pr[E_1] & (\text{Why?}) \\
 & \Pr[E_1|E_2] & = & \frac{\Pr[E_2|E_1]\times\Pr[E_1]}{\Pr[E_2]} & (\ldots)
\end{array}
$$

What type of proof is this?

Equivalence of definitions of perfect secrecy

Lemma 2.4 (Proved in textbook pg 30) $2.3(a) \Longrightarrow 2.3$

Fix M, m, c and noting that

$$\begin{aligned} \Pr[C = c | M = m] &= \Pr[\mathrm{Enc}_K(M) = c | M = m] \\ &= \Pr[\mathrm{Enc}_K(m) = c] \end{aligned}$$

And then $\Pr[M = m | C = c] \longrightarrow$ (using Bayes theorem) $\longrightarrow \Pr[M = m]$

$2.3 \Longrightarrow 2.3(a)$ **Prove here...**

Assuming 2.3, and we have perfect secrecy. Consider these steps for m:

$$\begin{array}{lrcll} & \Pr[M = m | C = c] & = & \frac{\Pr[C=c|M=m] \times \Pr[M=m]}{\Pr[C=c]} & (\text{Bayes}) \\ \text{and} & \Pr[M = m | C = c] & = & \Pr[M = m] & (\text{From 2.3}) \\ \text{so} & \Pr[C = c | M = m] & = & \Pr[C = c] & (\text{Why?}) \\ & \Pr[C = c | M = m] & = & \Pr[\mathrm{Enc}_k(m) = c] & (\text{Why?}) \end{array}$$

(i.e. $\Pr[\mathrm{Enc}_k(m) = c] = \Pr[C = c]$. We can do similar steps for m' to get $\Pr[C = c | M = m'] = \Pr[\mathrm{Enc}_k(m') = c] = \Pr[C = c]$. Given this we have that

$$\Pr[\mathrm{Enc}_k(m) = c] = \Pr[\mathrm{Enc}_k(m') = c]$$

■

Equivalence of definitions of perfect secrecy

Theorem 2.9: The (bitwise) one-time pad is perfectly secure

Proof:

1. show that for any m, c, $\Pr[\mathrm{Enc}_K(m) = c] = 2^{-\ell}$. Given that the key k is a uniform ℓ-bit string, then (from the book pg33):

$$\begin{aligned} \Pr[C = c | M = m] = \Pr[\mathrm{Enc}_k(m) = c] &= \Pr[m \oplus k = c] && \text{(Why?)} \\ &= \Pr[k = m \oplus c] && \text{(Why?)} \\ &= 2^{-\ell} && \text{(Why?)} \end{aligned}$$

2. Done already! Using Lemma 2.4 (equivalent of Def 2.3 and Def 2.3(a)). Re-work (1) above for m', and we have

$$\Pr[\mathrm{Enc}_k(m) = c] = \Pr[\mathrm{Enc}_k(m') = c] = 2^{-\ell}$$ ■

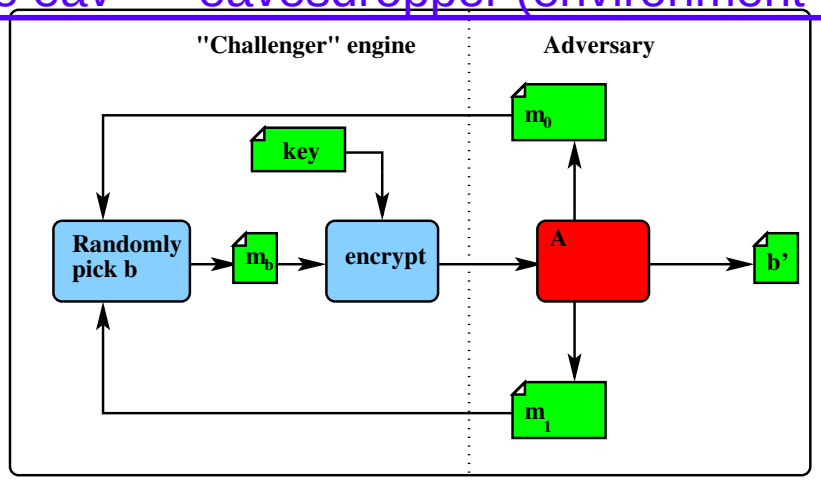
Textbook uses a different method, without using Lemma 2.4

An alternative (read modern) approach

Perfect (adversarial) indistinguishability

An adversarial "game" $\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$ which depends on the adversary and system algorithms $\mathcal{A}, \Pi$:

in this case the eav == eavesdropper (environment of the game)



1. Adversary chooses two (same length[a]) messages m_o, m_1
2. Challenger uniformly and randomly picks $b \in 0, 1$. Use Gen to pick a key k and obtain the challenge c, $c \leftarrow \mathrm{Enc}_k(m_b)$
3. On input c, Adversary A outputs a bit b'.
4. A succeeds if $b' = b$. In such case, we write $\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1$

[a] Textbook does not enforce this - a higher level!

Perfect (adversarial) indistinguishability is ...

Definition 2.5

Encryption Scheme Π is Perfectly Indistinguishable, if for any adversary $\mathcal{A}$,

$$\Pr[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}$$

use this definition to later find the expected returns

Lemma 2.6

An encryption scheme is perfectly indistinguishable iff it is perfectly secret.

Proof?... (perhaps later

A reminder of the bad news...

Theorem 2.10. If a scheme is perfectly secure, then $|\mathcal{K}| \geq |\mathcal{M}|$.

Akan Datang! How do we overcome it?

- Relax the requirements. Epsilon!
- Use not-so-perfect (computational) indistinguishability, and
- constrain the capability of the attacker.