17 de Abril de 2013, La Habana, Cuba

LOS USOS Y MAL USOS DE LA SIMULACIÓN MATEMÁTICA

Neal Koblitz
University of Washington, Seattle, U.S.A.,
koblitz@uw.edu

La simulación matemática quiere decir la solución de los problemas científicos, económicos, y sociales convirtiéndolos en problemas matemáticos.

La simulación matemática quiere decir la solución de los problemas científicos, económicos, y sociales convirtiéndolos en problemas matemáticos.

Algunas características típicas de la simulación matemática:

(1) A veces las matemáticas producen soluciones prácticas.

La simulación matemática quiere decir la solución de los problemas científicos, económicos, y sociales convirtiéndolos en problemas matemáticos.

Algunas características típicas de la simulación matemática:

(1) A veces las matemáticas producen soluciones prácticas.

(2) En la mayoría de los casos, los problemas sociales que pueden ser solucionados satisfactoriamente a través de las matemáticas son los problemas de menor importancia.

La simulación matemática quiere decir la solución de los problemas científicos, económicos, y sociales convirtiéndolos en problemas matemáticos.

Algunas características típicas de la simulación matemática:

(1) A veces las matemáticas producen soluciones prácticas.

(2) En la mayoría de los casos, los problemas sociales que pueden ser solucionados satisfactoriamente a través de las matemáticas son los problemas de menor importancia.

(3) Los problemas científicos que tienen una gran importancia social generalmente son muy difíciles para la simulación matemática.

Algunos ejemplos de problemas muy importantes (y muy difíciles) para la simulación matemática:

(1) la ecología

Algunos ejemplos de problemas muy importantes (y muy difíciles) para la simulación matemática:

(1) la ecología – los cambios del clima, la reclusión de carbono, el “tope e intercambio” (*cap and trade* en inglés), el impacto a largo plazo de los factores del estrés sobre los bosques, arrecifes, etcétera;

Algunos ejemplos de problemas muy importantes (y muy difíciles) para la simulación matemática:

(1) la ecología – los cambios del clima, la reclusión de carbono, el "tope e intercambio" (*cap and trade* en inglés), el impacto a largo plazo de los factores del estrés sobre los bosques, arrecifes, etcétera;

(2) los pronósticos meteorológicos;

Algunos ejemplos de problemas muy importantes (y muy difíciles) para la simulación matemática:

(1) la ecología – los cambios del clima, la reclusión de carbono, el "tope e intercambio" (*cap and trade* en inglés), el impacto a largo plazo de los factores del estrés sobre los bosques, arrecifes, etcétera;

(2) los pronósticos meteorológicos;

(3) las finanzas, la economía;

Algunos ejemplos de problemas muy importantes (y muy difíciles) para la simulación matemática:

(1) la ecología – los cambios del clima, la reclusión de carbono, el "tope e intercambio" (*cap and trade* en inglés), el impacto a largo plazo de los factores del estrés sobre los bosques, arrecifes, etcétera;

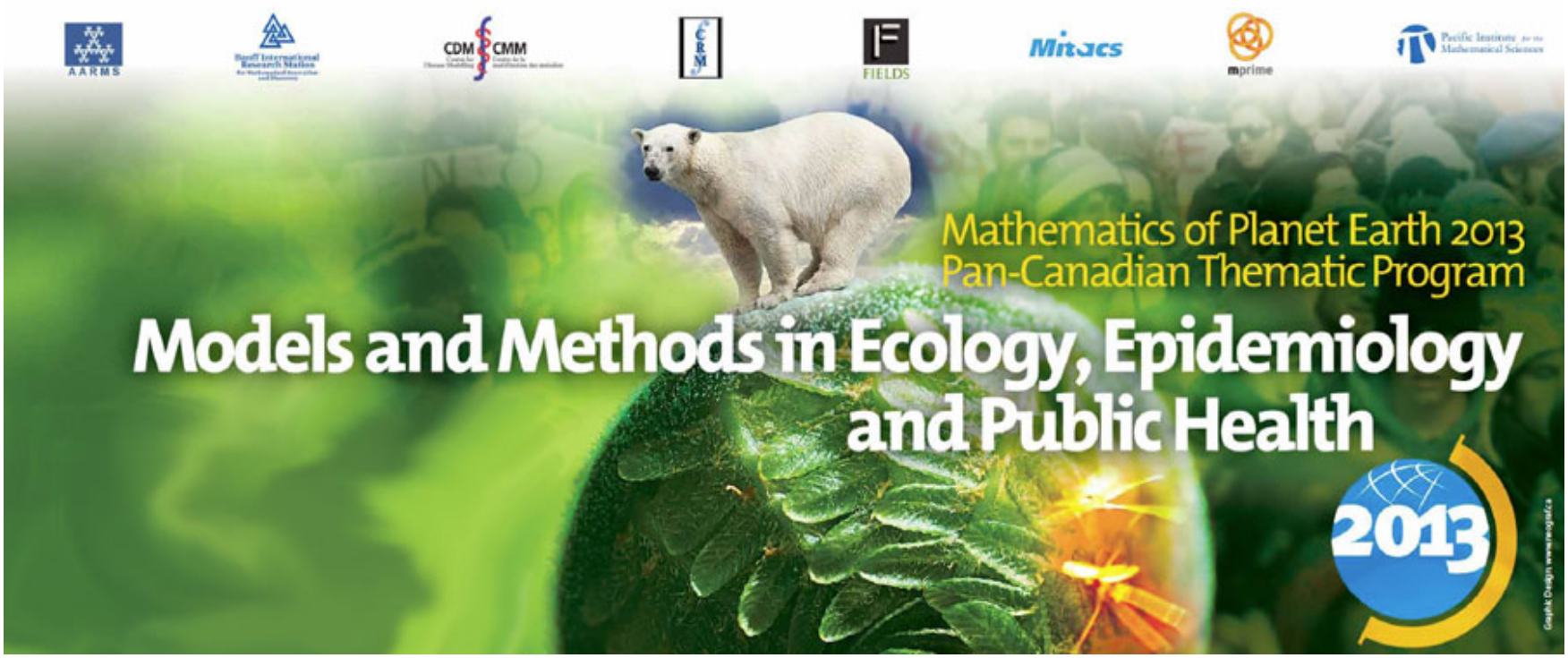
(2) los pronósticos meteorológicos;

(3) las finanzas, la economía;

(4) la seguridad de datos (mi campo de investigación).

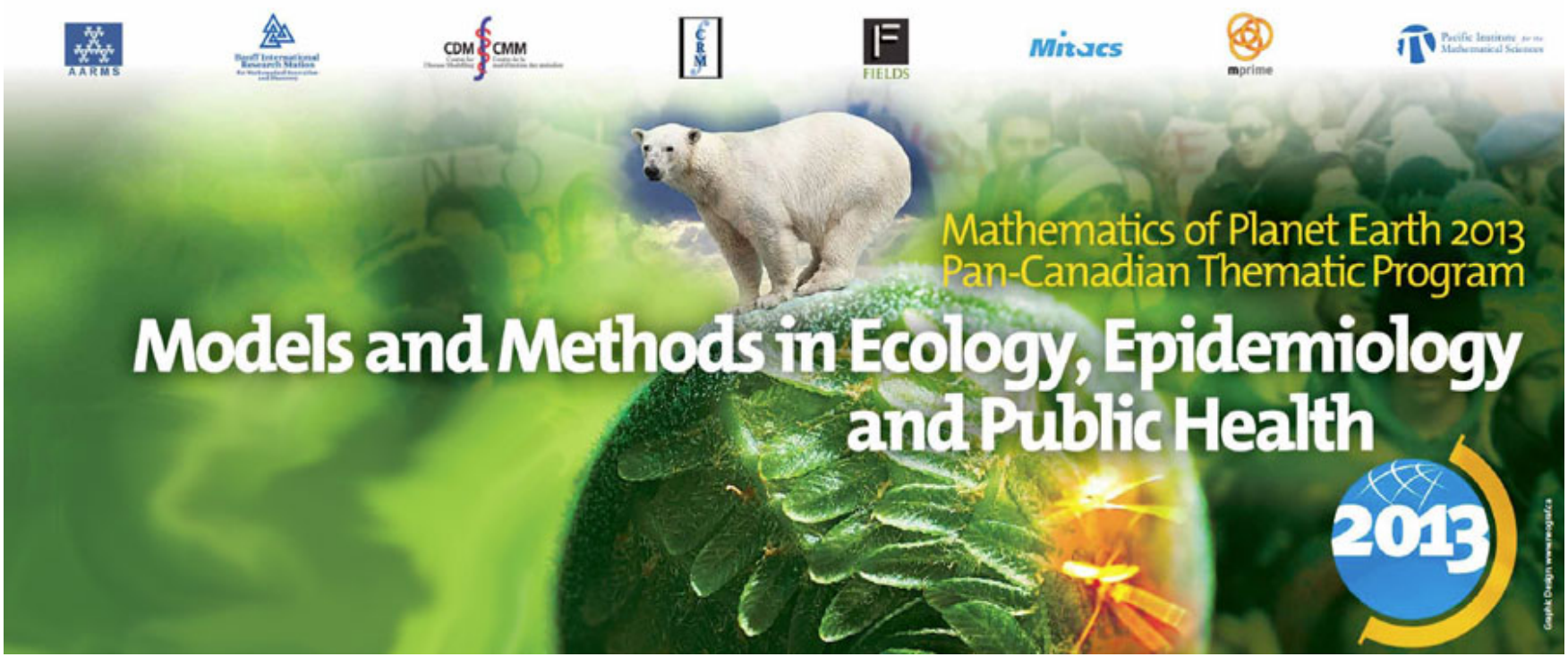
En la actualidad muchos especialistas en las ciencias matemáticas están trabajando en estos campos, y a veces han logrado algunos éxitos.

En la actualidad muchos especialistas en las ciencias matemáticas están trabajando en estos campos, y a veces han logrado algunos éxitos.



http://www.crm.math.ca/M2E2

En la actualidad muchos especialistas en las ciencias matemáticas están trabajando en estos campos, y a veces han logrado algunos éxitos.



http://www.crm.math.ca/M2E2

Pero mi enfoque en esta charla no va a ser los logros, sino los peligros de la simulación matemática.

Por un lado, los matemáticos podemos informar al público sobre las posibilidades de utilizar las matemáticas para solucionar problemas prácticos.

Por un lado, los matemáticos podemos informar al público sobre las posibilidades de utilizar las matemáticas para solucionar problemas prácticos.

Dos sugerencias:

(1)Paulatinamente introducir más problemas expresados en palabras cotidianas (donde el estudiante debe traducirlas al lenguaje de las matemáticas) en las asignaturas y los exámenes de entrada en las universidades.

Por un lado, los matemáticos podemos informar al público sobre las posibilidades de utilizar las matemáticas para solucionar problemas prácticos.

Dos sugerencias:

(1)Paulatinamente introducir más problemas expresados en palabras cotidianas (donde el estudiante debe traducirlas al lenguaje de las matemáticas) en las asignaturas y los exámenes de entrada en las universidades.

A menudo los jóvenes consideran las matemáticas nada más que un obstáculo que deben superar para ingresar en la universidad.

Por un lado, los matemáticos podemos informar al público sobre las posibilidades de utilizar las matemáticas para solucionar problemas prácticos.

Dos sugerencias:

(1)Paulatinamente introducir más problemas expresados en palabras cotidianas (donde el estudiante debe traducirlas al lenguaje de las matemáticas) en las asignaturas y los exámenes de entrada en las universidades.

A menudo los jóvenes consideran las matemáticas nada más que un obstáculo que deben superar para ingresar en la universidad. Debemos enseñar que las matemáticas son una herramienta valiosa para cualquier científico, ingeniero, o ciudadano inteligente.

(2) Cuba podría tener equipos en el Concurso Matemático en la Simulación (*Mathematical Contest in Modeling* http://www.comap.com/undergraduate/ contests/mcm/ instructions.php)

(2) Cuba podría tener equipos en el Concurso Matemático en la Simulación (*Mathematical Contest in Modeling* http://www.comap.com/undergraduate/ contests/mcm/ instructions.php)

Este concurso es muy diferente de la Olimpíada Matemática Internacional:

(2) Cuba podría tener equipos en el Concurso Matemático en la Simulación (*Mathematical Contest in Modeling* http://www.comap.com/undergraduate/ contests/mcm/ instructions.php)

Este concurso es muy diferente de la Olimpíada Matemática Internacional:

(a) está en el Internet, no en reuniones físicas;

(b) por eso no es costoso (US$100 para inscribir un equipo);

(2) Cuba podría tener equipos en el Concurso Matemático en la Simulación (*Mathematical Contest in Modeling* http://www.comap.com/undergraduate/ contests/mcm/ instructions.php)

Este concurso es muy diferente de la Olimpíada Matemática Internacional:

(a) está en el Internet, no en reuniones físicas;

(b) por eso no es costoso (US$100 para inscribir un equipo);

(c) participan estudiantes universitarios, no de los colegios;

(2) Cuba podría tener equipos en el Concurso Matemático en la Simulación (*Mathematical Contest in Modeling* http://www.comap.com/undergraduate/ contests/mcm/ instructions.php)

Este concurso es muy diferente de la Olimpíada Matemática Internacional:

(a) está en el Internet, no en reuniones físicas;

(b) por eso no es costoso (US$100 para inscribir un equipo);

(c) participan estudiantes universitarios, no de los colegios;

(d) pueden participar varios equipos del mismo país (en general de diferentes universidades) – un gran número de equipos provienen de los Estados Unidos y China;

(2) Cuba podría tener equipos en el Concurso Matemático en la Simulación (*Mathematical Contest in Modeling* http://www.comap.com/undergraduate/ contests/mcm/ instructions.php)

Este concurso es muy diferente de la Olimpíada Matemática Internacional:

(a) está en el Internet, no en reuniones físicas;

(b) por eso no es costoso (US$100 para inscribir un equipo);

(c) participan estudiantes universitarios, no de los colegios;

(d) pueden participar varios equipos del mismo país (en general de diferentes universidades) – un gran número de equipos provienen de los Estados Unidos y China;

(e) cada equipo debe solucionar no 6 problemas de las matemáticas puras, sino 1 problema práctico;

(2) Cuba podría tener equipos en el Concurso Matemático en la Simulación (*Mathematical Contest in Modeling* http://www.comap.com/undergraduate/ contests/mcm/ instructions.php)

Este concurso es muy diferente de la Olimpíada Matemática Internacional:

(a) está en el Internet, no en reuniones físicas;
(b) por eso no es costoso (US$100 para inscribir un equipo);
(c) participan estudiantes universitarios, no de los colegios;
(d) pueden participar varios equipos del mismo país (en general de diferentes universidades) – un gran número de equipos provienen de los Estados Unidos y China;
(e) cada equipo debe solucionar no 6 problemas de las matemáticas puras, sino 1 problema práctico;
(f) trabajan en equipo, no individualmente.

Además de enseñar a la juventud sobre los usos prácticos de las matemáticas, debemos también educar al público sobre lo que las matemáticas no pueden hacer.

Además de enseñar a la juventud sobre los usos prácticos de las matemáticas, debemos también educar al público sobre lo que las matemáticas no pueden hacer.

A veces el papel más importante que puede jugar un matemático es criticar los usos no apropiados de las matemáticas.

Además de enseñar a la juventud sobre los usos prácticos de las matemáticas, debemos también educar al público sobre lo que las matemáticas no pueden hacer.

A veces el papel más importante que puede jugar un matemático es criticar los usos no apropiados de las matemáticas. Puede ser más útil que el desarrollar los usos correctos.

Además de enseñar a la juventud sobre los usos prácticos de las matemáticas, debemos también educar al público sobre lo que las matemáticas no pueden hacer.

A veces el papel más importante que puede jugar un matemático es criticar los usos no apropiados de las matemáticas. Puede ser más útil que el desarrollar los usos correctos.

Una situación análoga: Una de las tareas de la profesión médica es combatir las "curas" fraudulentas y educar al público sobre los tratamientos falsos.

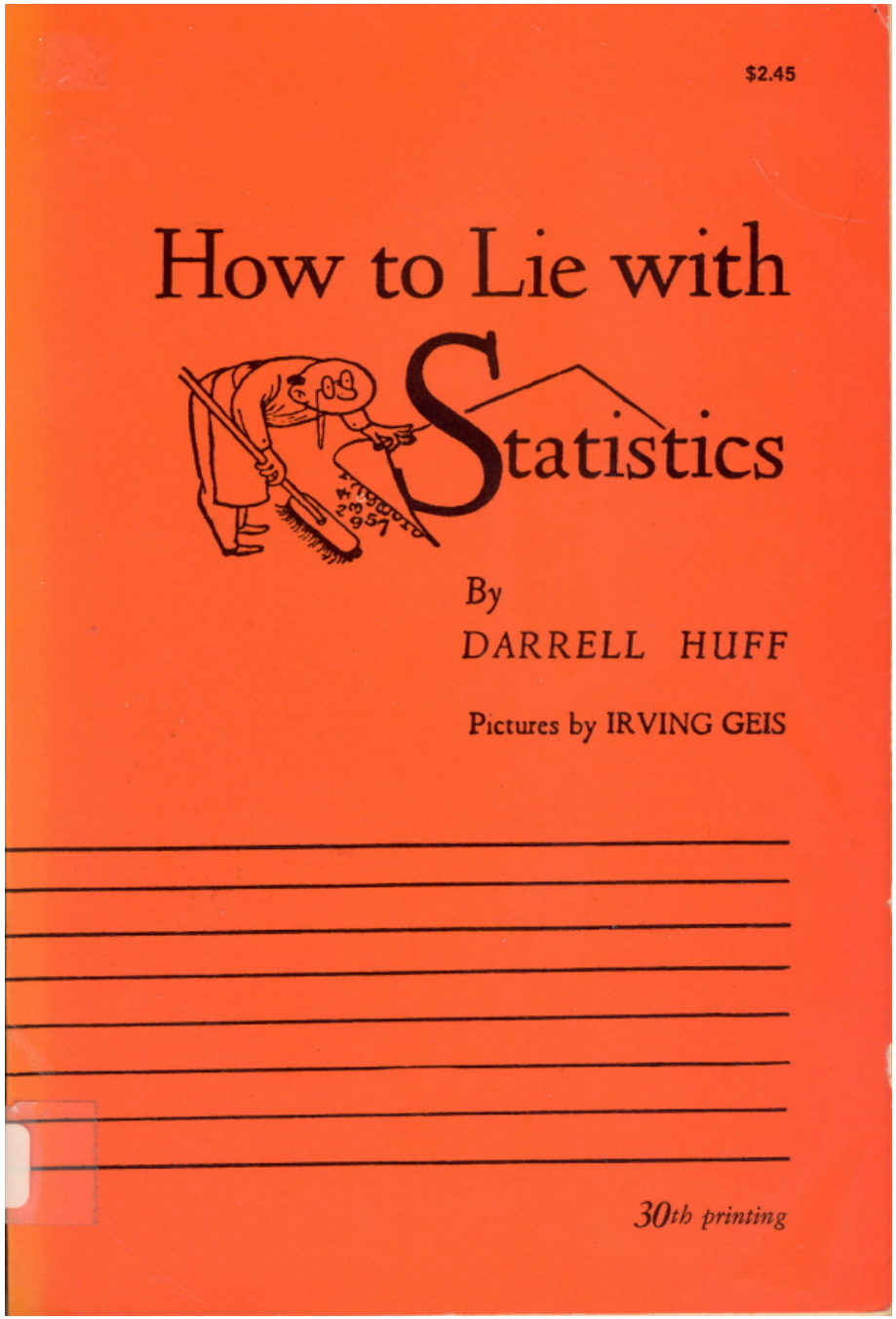
Además de enseñar a la juventud sobre los usos prácticos de las matemáticas, debemos también educar al público sobre lo que las matemáticas no pueden hacer.

A veces el papel más importante que puede jugar un matemático es criticar los usos no apropiados de las matemáticas. Puede ser más útil que el desarrollar los usos correctos.

Una situación análoga: Una de las tareas de la profesión médica es combatir las "curas" fraudulentas y educar al público sobre los tratamientos falsos.

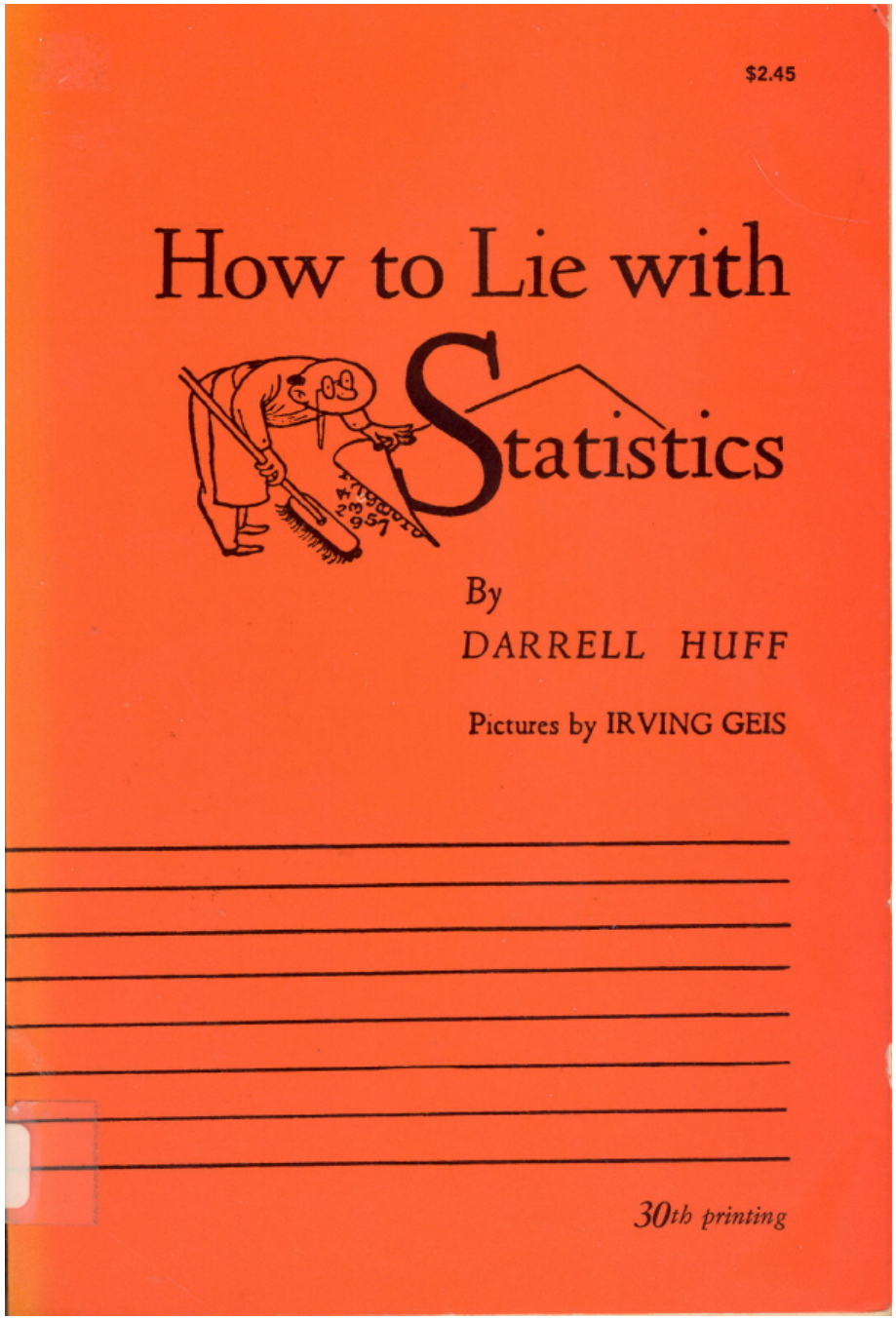
De una manera semejante los matemáticos podemos explicar, por ejemplo, los usos distorsionados de las estadísticas.

El libro clásico “Como mentir con las estadísticas,” publicado por primera vez en 1954.



El libro clásico “Como mentir con las estadísticas,” publicado por primera vez en 1954.

Con claridad y humor se explican algunos de los métodos usados para engañar al público a través de las estadísticas.



Existen muchas maneras de mentir con las estadísticas, incluyendo algunas que no son examinadas en este libro.

Existen muchas maneras de mentir con las estadísticas, incluyendo algunas que no son examinadas en este libro.

Es fácil engañar al público, ya que mucha gente creen que la información cuantitativa es más confiable que la cualitativa.

Existen muchas maneras de mentir con las estadísticas, incluyendo algunas que no son examinadas en este libro.

Es fácil engañar al público, ya que mucha gente creen que la información cuantitativa es más confiable que la cualitativa. Es decir, creen que “los números no mienten.”

Existen muchas maneras de mentir con las estadísticas, incluyendo algunas que no son examinadas en este libro.

Es fácil engañar al público, ya que mucha gente creen que la información cuantitativa es más confiable que la cualitativa. Es decir, creen que “los números no mienten.”

A continuación sigue un ejemplo de las estadísticas mentirosas que proviene de Vietnam

Existen muchas maneras de mentir con las estadísticas, incluyendo algunas que no son examinadas en este libro.

Es fácil engañar al público, ya que mucha gente creen que la información cuantitativa es más confiable que la cualitativa. Es decir, creen que "los números no mienten."

A continuación sigue un ejemplo de las estadísticas mentirosas que proviene de Vietnam – más bien, de un oficial norteamericano que vive en Vietnam.

Table 1. Publications in Peer-Review Journals, 2007

Institution	Country	Publications
Seoul Natl. University	Republic of Korea	5,060
….	….	….
University of Philippines	Philippines	220
Vietnam Nat. University (Hanoi and HCMC)	Vietnam	52
Vietnam Academy of Science and Technology	Vietnam	44

Source: Science Citation Index Expanded, Thomson Reuters

Table 1. Publications in Peer-Review Journals, 2007

Institution	Country	Publications
Seoul Natl. University	Republic of Korea	5,060
….	….	….
University of Philippines	Philippines	220
Vietnam Nat. University (Hanoi and HCMC)	Vietnam	52
Vietnam Academy of Science and Technology	Vietnam	44

Source: Science Citation Index Expanded, Thomson Reuters

Esta tabla se encuentra en la pag. 2 del informe del Sr. Thomas Vallely (quien es director del Programa Fulbright en Vietnam) que escribió para la Fuerza de Tarea en la Educación Superior (*U.S.-Vietnam Higher Education Task Force*).

Table 1. Publications in Peer-Review Journals, 2007

Institution	Country	Publications
Seoul Natl. University	Republic of Korea	5,060
….	….	….
University of Philippines	Philippines	220
Vietnam Nat. University (Hanoi and HCMC)	Vietnam	52
Vietnam Academy of Science and Technology	Vietnam	44

Source: Science Citation Index Expanded, Thomson Reuters

Esta tabla se encuentra en la pag. 2 del informe del Sr. Thomas Vallely (quien es director del Programa Fulbright en Vietnam) que escribió para la Fuerza de Tarea en la Educación Superior (*U.S.-Vietnam Higher Education Task Force*). Es de notar que el informe de Vallely fue publicado en vietnamita en uno de los periódicos más populares, el *Tuổi Trẻ.*

Muchos vietnamitas fueron engañados por esta tabla.
“No podemos disputar los números.

Muchos vietnamitas fueron engañados por esta tabla. “No podemos disputar los números. Parece horrible, pero este norteamericano debe saber la verdad.”

Muchos vietnamitas fueron engañados por esta tabla. “No podemos disputar los números. Parece horrible, pero este norteamericano debe saber la verdad.”

Los lectores más enterados pudieron decir, “Eso es tonterías.

Muchos vietnamitas fueron engañados por esta tabla. “No podemos disputar los números. Parece horrible, pero este norteamericano debe saber la verdad.”

Los lectores más enterados pudieron decir, “Eso es tonterías. Obviamente, casi todos los científicos en la Academia de Ciencia y Tecnología (VAST) indican el nombre de su instituto específico en sus trabajos, no el nombre de VAST.”

Muchos vietnamitas fueron engañados por esta tabla. “No podemos disputar los números. Parece horrible, pero este norteamericano debe saber la verdad.”

Los lectores más enterados pudieron decir, “Eso es tonterías. Obviamente, casi todos los científicos en la Academia de Ciencia y Tecnología (VAST) indican el nombre de su instituto específico en sus trabajos, no el nombre de VAST.”

Yo tengo un listado de las publicaciones del Instituto de Matemáticas de Hanoi durante el período 1970—2000, el cual contiene casi 2000 artículos.

Muchos vietnamitas fueron engañados por esta tabla. “No podemos disputar los números. Parece horrible, pero este norteamericano debe saber la verdad.”

Los lectores más enterados pudieron decir, “Eso es tonterías. Obviamente, casi todos los científicos en la Academia de Ciencia y Tecnología (VAST) indican el nombre de su instituto específico en sus trabajos, no el nombre de VAST.”

Yo tengo un listado de las publicaciones del Instituto de Matemáticas de Hanoi durante el período 1970—2000, el cual contiene casi 2000 artículos. Y la Academia (VAST) consiste en más de 30 institutos.

Muchos vietnamitas fueron engañados por esta tabla. “No podemos disputar los números. Parece horrible, pero este norteamericano debe saber la verdad.”

Los lectores más enterados pudieron decir, “Eso es tonterías. Obviamente, casi todos los científicos en la Academia de Ciencia y Tecnología (VAST) indican el nombre de su instituto específico en sus trabajos, no el nombre de VAST.”

Yo tengo un listado de las publicaciones del Instituto de Matemáticas de Hanoi durante el período 1970—2000, el cual contiene casi 2000 artículos. Y la Academia (VAST) consiste en más de 30 institutos. Es claro que las estadísticas del Sr. Vallely son absurdas.

El informe de Vallely contenía muchos insultos y desinformación dirigidos contra la comunidad científica vietnamita y los oficiales universitarios.

El informe de Vallely contenía muchos insultos y desinformación dirigidos contra la comunidad científica vietnamita y los oficiales universitarios. Vallely tenía dos motivos:

El informe de Vallely contenía muchos insultos y desinformación dirigidos contra la comunidad científica vietnamita y los oficiales universitarios. Vallely tenía dos motivos:

(1) Convencer al público que la ciencia y la educación en Vietnam están en un nivel muy bajo,

El informe de Vallely contenía muchos insultos y desinformación dirigidos contra la comunidad científica vietnamita y los oficiales universitarios. Vallely tenía dos motivos:

(1) Convencer al público que la ciencia y la educación en Vietnam están en un nivel muy bajo, y que Vietnam debe pagar a un grupo de norteamericanos más de US$$10^8$ para construir una universidad nueva en Vietnam (usando un préstamo muy grande del Banco Mundial para conseguir este dinero que debe ser enviado a los Estados Unidos).

El informe de Vallely contenía muchos insultos y desinformación dirigidos contra la comunidad científica vietnamita y los oficiales universitarios. Vallely tenía dos motivos:

(1) Convencer al público que la ciencia y la educación en Vietnam están en un nivel muy bajo, y que Vietnam debe pagar a un grupo de norteamericanos más de US$$10^8$ para construir una universidad nueva en Vietnam (usando un préstamo muy grande del Banco Mundial para conseguir este dinero que debe ser enviado a los Estados Unidos).

(2) Fomentar una actitud negativa y cínica respecto a los logros del socialismo vietnamita, especialmente entre los jóvenes.

El informe de Vallely contenía muchos insultos y desinformación dirigidos contra la comunidad científica vietnamita y los oficiales universitarios. Vallely tenía dos motivos:

(1) Convencer al público que la ciencia y la educación en Vietnam están en un nivel muy bajo, y que Vietnam debe pagar a un grupo de norteamericanos más de US$$10^8$ para construir una universidad nueva en Vietnam (usando un préstamo muy grande del Banco Mundial para conseguir este dinero que debe ser enviado a los Estados Unidos).

(2) Fomentar una actitud negativa y cínica respecto a los logros del socialismo vietnamita, especialmente entre los jóvenes. (El periódico que tradujo el informe de Vallely está dirigido hacia la juventud.)

El mal uso de las matemáticas no necesariamente toma la forma de “mentir con las estadísticas.”

El mal uso de las matemáticas no necesariamente toma la forma de “mentir con las estadísticas.”

En los años 1970 mi esposa Ann era estudiante de posgrado en historia. Uno de los artículos que tuvo que leer durante un seminario fue escrito por el especialista en la “ciencia” política Samuel Huntington.

El mal uso de las matemáticas no necesariamente toma la forma de “mentir con las estadísticas.”

En los años 1970 mi esposa Ann era estudiante de posgrado en historia. Uno de los artículos que tuvo que leer durante un seminario fue escrito por el especialista en la “ciencia” política Samuel Huntington. El usó tres ecuaciones matemáticas de la forma $a = b/c$ para simular el comportamiento político en una sociedad.

El mal uso de las matemáticas no necesariamente toma la forma de “mentir con las estadísticas.”

En los años 1970 mi esposa Ann era estudiante de posgrado en historia. Uno de los artículos que tuvo que leer durante un seminario fue escrito por el especialista en la “ciencia” política Samuel Huntington. El usó tres ecuaciones matemáticas de la forma $a = b/c$ para simular el comportamiento político en una sociedad. Por ejemplo:

frustración social / oportunidades de movilidad social
= participación política

El mal uso de las matemáticas no necesariamente toma la forma de “mentir con las estadísticas.”

En los años 1970 mi esposa Ann era estudiante de posgrado en historia. Uno de los artículos que tuvo que leer durante un seminario fue escrito por el especialista en la “ciencia” política Samuel Huntington. El usó tres ecuaciones matemáticas de la forma a = b/c para simular el comportamiento político en una sociedad. Por ejemplo:

frustración social / oportunidades de movilidad social
= participación política

y

participación política / institucionalización política
= inestabilidad política

Ann comentó correctamente que la simulación no tenía validez alguna, sino fue usada para impresionar e intimidar (ya que la mayoría de los lectores del artículo no entendían nada de las matemáticas).

Ann comentó correctamente que la simulación no tenía validez alguna, sino fue usada para impresionar e intimidar (ya que la mayoría de los lectores del artículo no entendían nada de las matemáticas).

En 1981 publiqué un artículo que, entre otras cosas, criticó las ecuaciones de Huntington.

Ann comentó correctamente que la simulación no tenía validez alguna, sino fue usada para impresionar e intimidar (ya que la mayoría de los lectores del artículo no entendían nada de las matemáticas).

En 1981 publiqué un artículo que, entre otras cosas, criticó las ecuaciones de Huntington.

Envié una copia de mi artículo al matemático muy conocido Serge Lang, quien a veces se había opuesto al uso de los métodos falaces en las investigaciones académicas.

En 1986 Serge Lang utilizó mi artículo para oponerse a la elección de Samuel Huntington como miembro de la Academia de Ciencias norteamericana. Los científicos votaron en contra de Huntington debido a su mal uso de las matemáticas.

En 1986 Serge Lang utilizó mi artículo para oponerse a la elección de Samuel Huntington como miembro de la Academia de Ciencias norteamericana. Los científicos votaron en contra de Huntington debido a su mal uso de las matemáticas. Esta votación recibió mucha publicidad en la prensa norteamericana (un artículo en la primera página del *New York Times*). El era profesor en la Univ. de Harvard, y había sido oficial de alto rango en el gobierno de los EEUU.

En 1986 Serge Lang utilizó mi artículo para oponerse a la elección de Samuel Huntington como miembro de la Academia de Ciencias norteamericana. Los científicos votaron en contra de Huntington debido a su mal uso de las matemáticas. Esta votación recibió mucha publicidad en la prensa norteamericana (un artículo en la primera página del *New York Times*). El era profesor en la Univ. de Harvard, y había sido oficial de alto rango en el gobierno de los EEUU.

Serge Lang y yo estuvimos muy contentos de haber prevenido la elección de Huntington en parte debido al papel que había jugado en la guerra contra Vietnam.

En 1986 Serge Lang utilizó mi artículo para oponerse a la elección de Samuel Huntington como miembro de la Academia de Ciencias norteamericana. Los científicos votaron en contra de Huntington debido a su mal uso de las matemáticas. Esta votación recibió mucha publicidad en la prensa norteamericana (un artículo en la primera página del *New York Times*). El era profesor en la Univ. de Harvard, y había sido oficial de alto rango en el gobierno de los EEUU.

Serge Lang y yo estuvimos muy contentos de haber prevenido la elección de Huntington en parte debido al papel que había jugado en la guerra contra Vietnam. El había dirigido el desarrollo del programa "aldeas estratégicas" ("*strategic hamlets*" en inglés – el traslado forzado de pueblos vietnamitas)

En 1986 Serge Lang utilizó mi artículo para oponerse a la elección de Samuel Huntington como miembro de la Academia de Ciencias norteamericana. Los científicos votaron en contra de Huntington debido a su mal uso de las matemáticas. Esta votación recibió mucha publicidad en la prensa norteamericana (un artículo en la primera página del *New York Times*). El era profesor en la Univ. de Harvard, y había sido oficial de alto rango en el gobierno de los EEUU.

Serge Lang y yo estuvimos muy contentos de haber prevenido la elección de Huntington en parte debido al papel que había jugado en la guerra contra Vietnam. El había dirigido el desarrollo del programa "aldeas estratégicas" ("*strategic hamlets*" en inglés – el traslado forzado de pueblos vietnamitas) el cual fue una violación del Artículo 49 de la Cuarta Convención de Ginebra sobre crímenes de guerra.

El Caso de la Simulación Matemática Más Desastrosa en Toda la Historia

En 2000, David Li (quien es chino-canadiense con un doctorado de la Universidad de Waterloo) diseñó una simulación para predecir la probabilidad de que un conjunto dado de compañías una tras otra tengan incumplimiento de sus deudas de bonos.

El Caso de la Simulación Matemática Más Desastrosa en Toda la Historia

En 2000, David Li (quien es chino-canadiense con un doctorado de la Universidad de Waterloo) diseñó una simulación para predecir la probabilidad de que un conjunto dado de compañías una tras otra tengan incumplimiento de sus deudas de bonos.

El Caso de la Simulación Matemática Más Desastrosa en Toda la Historia

En 2000, David Li (quien es chino-canadiense con un doctorado de la Universidad de Waterloo) diseñó una simulación para predecir la probabilidad de que un conjunto dado de compañías una tras otra tengan incumplimiento de sus deudas de bonos.

Según *The Wall Street Journal* (2005):

"La simulación matemática alimentó el crecimiento explosivo del mercado de lo que se llama derivados de crédito…. Este mercado apenas existía en los años 1990. En la

actualidad este mercado es tan gigantesco… y tan turbio que ha causado expresiones de inquietud de parte de algunos observadores de la bolsa….”

actualidad este mercado es tan gigantesco… y tan turbio que ha causado expresiones de inquietud de parte de algunos observadores de la bolsa….”

Dinero invertido en “canjes de crédito incumplido” (CDO – obligaciones de deuda colateralizada/garantizada):

actualidad este mercado es tan gigantesco… y tan turbio que ha causado expresiones de inquietud de parte de algunos observadores de la bolsa….”

Dinero invertido en “canjes de crédito incumplido” (CDO – obligaciones de deuda colateralizada/garantizada):

2001: $920,000 millones

actualidad este mercado es tan gigantesco… y tan turbio que ha causado expresiones de inquietud de parte de algunos observadores de la bolsa….”

Dinero invertido en “canjes de crédito incumplido” (CDO – obligaciones de deuda colateralizada/garantizada):

2001: $920,000 millones

2007: $62,000,000 millones

actualidad este mercado es tan gigantesco… y tan turbio que ha causado expresiones de inquietud de parte de algunos observadores de la bolsa….”

Dinero invertido en “canjes de crédito incumplido” (CDO – obligaciones de deuda colateralizada/garantizada):

2001: $920,000 millones

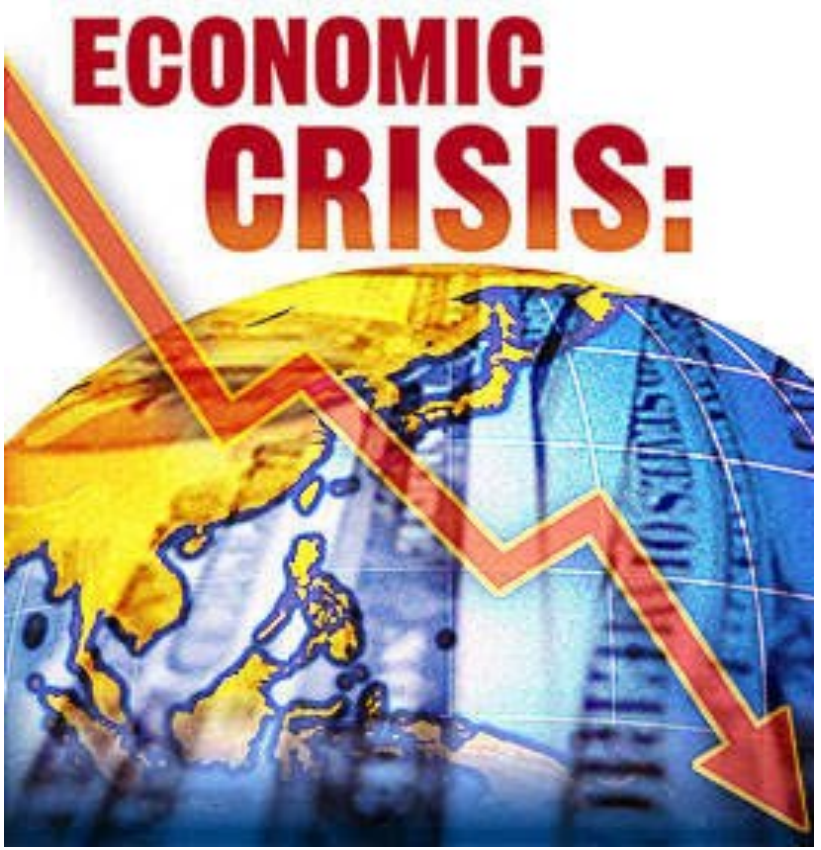
2007: $62,000,000 millones

En el transcurso de 6 años la cantidad de dinero invertido en los “derivados’’ exóticos y riesgosos se duplicó 6 veces de US$ 2^{40} a US$ 2^{46}.

A pesar de las garantías que resultaron de la simulación de David Li, en 2008 este mercado se derrumbó,

A pesar de las garantías que resultaron de la simulación de David Li, en 2008 este mercado se derrumbó, lo cual condujo a la crisis económica mundial de los últimos 5 años — la peor crisis del capitalismo desde los años 1930.

A pesar de las garantías que resultaron de la simulación de David Li, en 2008 este mercado se derrumbó, lo cual condujo a la crisis económica mundial de los últimos 5 años — la peor crisis del capitalismo desde los años 1930.



Los ejemplos de Samuel Huntington y de David Li son casos extremos. La mayoría de los que usan las matemáticas de una manera distorsionada no son criminales de guerra, y no contribuyen a la creación de una crisis económica mundial.

Los ejemplos de Samuel Huntington y de David Li son casos extremos. La mayoría de los que usan las matemáticas de una manera distorsionada no son criminales de guerra, y no contribuyen a la creación de una crisis económica mundial. Las discusiones sobre el mal uso de las matemáticas muy pocas veces se encuentran en las primeras páginas de los periódicos.

Los ejemplos de Samuel Huntington y de David Li son casos extremos. La mayoría de los que usan las matemáticas de una manera distorsionada no son criminales de guerra, y no contribuyen a la creación de una crisis económica mundial. Las discusiones sobre el mal uso de las matemáticas muy pocas veces se encuentran en las primeras páginas de los periódicos.

Algunas de las deficiencias más comunes en la simulación matemática:

(1)es demasiado simplificada;

Los ejemplos de Samuel Huntington y de David Li son casos extremos. La mayoría de los que usan las matemáticas de una manera distorsionada no son criminales de guerra, y no contribuyen a la creación de una crisis económica mundial. Las discusiones sobre el mal uso de las matemáticas muy pocas veces se encuentran en las primeras páginas de los periódicos.

Algunas de las deficiencias más comunes en la simulación matemática:

(1)es demasiado simplificada;
(2)está basada en suposiciones poco realistas;

Los ejemplos de Samuel Huntington y de David Li son casos extremos. La mayoría de los que usan las matemáticas de una manera distorsionada no son criminales de guerra, y no contribuyen a la creación de una crisis económica mundial. Las discusiones sobre el mal uso de las matemáticas muy pocas veces se encuentran en las primeras páginas de los periódicos.

Algunas de las deficiencias más comunes en la simulación matemática:

(1)es demasiado simplificada;
(2)está basada en suposiciones poco realistas;
(3)tiene suposiciones no explícitas (inconscientes);

Los ejemplos de Samuel Huntington y de David Li son casos extremos. La mayoría de los que usan las matemáticas de una manera distorsionada no son criminales de guerra, y no contribuyen a la creación de una crisis económica mundial. Las discusiones sobre el mal uso de las matemáticas muy pocas veces se encuentran en las primeras páginas de los periódicos.

Algunas de las deficiencias más comunes en la simulación matemática:

(1)es demasiado simplificada;
(2)está basada en suposiciones poco realistas;
(3)tiene suposiciones no explícitas (inconscientes);
(4)hasta errores pequeños en las suposiciones o los datos pueden causar errores grandes en los resultados.

Casos Problemáticos de la Simulación Matemática en la Criptografía

En 2011 en la CUJAE hablé sobre algunas deficiencias en la definición ampliamente aceptada de lo que quiere decir un sistema de firma digital “seguro.”

Casos Problemáticos de la Simulación Matemática en la Criptografía

En 2011 en la CUJAE hablé sobre algunas deficiencias en la definición ampliamente aceptada de lo que quiere decir un sistema de firma digital “seguro.”
Expliqué que una firma supuestamente “segura” podría ser muy vulnerable a los ataques del tipo “clave seleccionada para firma duplicada.”

Casos Problemáticos de la Simulación Matemática en la Criptografía

En 2011 en la CUJAE hablé sobre algunas deficiencias en la definición ampliamente aceptada de lo que quiere decir un sistema de firma digital “seguro.”
Expliqué que una firma supuestamente “segura” podría ser muy vulnerable a los ataques del tipo “clave seleccionada para firma duplicada.”

En otras palabras, la simulación matemática aceptada del concepto cotidiano de una “firma segura” no es completamente adecuada.

Hoy quiero explicar otro ejemplo de una simulación matemática en la criptografía que, aunque tiene muchos seguidores y defensores, es falaz.

Hoy quiero explicar otro ejemplo de una simulación matemática en la criptografía que, aunque tiene muchos seguidores y defensores, es falaz.

Este ejemplo tiene que ver con la criptografía simétrica (no la de clave pública).

Hoy quiero explicar otro ejemplo de una simulación matemática en la criptografía que, aunque tiene muchos seguidores y defensores, es falaz.

Este ejemplo tiene que ver con la criptografía simétrica (no la de clave pública).

Definición. Un código de autenticación de mensajes (MAC) es un sistema en que dos usuarios que comparten una clave secreta pueden intercambiar mensajes verificando que cada mensaje recibido es idéntico al mensaje enviado por el otro usuario.

Hoy quiero explicar otro ejemplo de una simulación matemática en la criptografía que, aunque tiene muchos seguidores y defensores, es falaz.

Este ejemplo tiene que ver con la criptografía simétrica (no la de clave pública).

Definición. Un código de autenticación de mensajes (MAC) es un sistema en que dos usuarios que comparten una clave secreta pueden intercambiar mensajes verificando que cada mensaje recibido es idéntico al mensaje enviado por el otro usuario.

El MAC más ampliamente usado se llama HMAC – está basado en una *función de compresión.*

Consideremos una función de compresión

$f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c , \quad b > c.$

Consideremos una función de compresión

$f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c$, $b > c$.

Típicamente $b=512$ y $c=160$ o 128.

Consideremos una función de compresión

$f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c$, $b > c$.

Típicamente $b=512$ y $c=160$ o 128.

Se usa para la construcción del sistema HMAC para la autenticación de mensajes.

Consideremos una función de compresión

$f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c$, $b > c$.

Típicamente $b=512$ y $c=160$ o 128.

Se usa para la construcción del sistema HMAC para la autenticación de mensajes. Por ejemplo, la etiqueta de un mensaje (M_1,M_2,M_3) de 3b bits es más o menos

$$f(K', f(f(f(K,M_1),M_2),M_3)).$$

Consideremos una función de compresión

$f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c, \quad b > c.$

Típicamente $b=512$ y $c=160$ o 128.

Se usa para la construcción del sistema HMAC para la autenticación de mensajes. Por ejemplo, la etiqueta de un mensaje (M_1,M_2,M_3) de $3b$ bits es más o menos

$$f(K', f(f(f(K,M_1),M_2),M_3)).$$

(Para más detalles: http://anotherlook.ca
"Another Look at HMAC")

En la conferencia Crypto 2006, Mihir Bellare presentó una demostración nueva de la seguridad de HMAC – en el sentido fuerte de la propiedad “pseudo-aleatoria” – con el hipótesis de que la función f es pseudo-aleatoria

En la conferencia Crypto 2006, Mihir Bellare presentó una demostración nueva de la seguridad de HMAC – en el sentido fuerte de la propiedad “pseudo-aleatoria” – con el hipótesis de que la función f es pseudo-aleatoria (sin ningúna suposición sobre la resistencia a choques).

En la conferencia Crypto 2006, Mihir Bellare presentó una demostración nueva de la seguridad de HMAC – en el sentido fuerte de la propiedad “pseudo-aleatoria” – con el hipótesis de que la función f es pseudo-aleatoria (sin ningúna suposición sobre la resistencia a choques).

El teorema de Bellare:

Si f es pseudo-aleatoria, entonces HMAC lo es también.

En la conferencia Crypto 2006, Mihir Bellare presentó una demostración nueva de la seguridad de HMAC – en el sentido fuerte de la propiedad "pseudo-aleatoria" – con el hipótesis de que la función f es pseudo-aleatoria (sin ningúna suposición sobre la resistencia a choques).

El teorema de Bellare:

Si f es pseudo-aleatoria, entonces HMAC lo es también.

Bellare aseguró que su teorema justifica el HMAC "hasta alrededor de $2^{c/2}/n$ preguntas," donde n es el número máximo de bloques en el mensaje, digamos, $n = 2^{20}$.

En la conferencia Crypto 2006, Mihir Bellare presentó una demostración nueva de la seguridad de HMAC – en el sentido fuerte de la propiedad "pseudo-aleatoria" – con el hipótesis de que la función f es pseudo-aleatoria (sin ningúna suposición sobre la resistencia a choques).

El teorema de Bellare:

Si f es pseudo-aleatoria, entonces HMAC lo es también.

Bellare aseguró que su teorema justifica el HMAC "hasta alrededor de $2^{c/2}/n$ preguntas," donde n es el número máximo de bloques en el mensaje, digamos, $n = 2^{20}$. Es decir, 2^{44} preguntas cuando c=128 y 2^{60} preguntas cuando c=160.

Definición de la seguridad pseudo-aleatoria.

Recordemos que $f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c$. Tenemos $T=f(K,M)$, donde T es la etiqueta de c bits determinada por la clave K de c bits y el mensaje M de b bits.

Definición de la seguridad pseudo-aleatoria.

Recordemos que $f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c$. Tenemos $T=f(K,M)$, donde T es la etiqueta de c bits determinada por la clave K de c bits y el mensaje M de b bits.

Al adversario A se le presenta un oráculo O que, cuando A le da una pregunta-mensaje, genera una respuesta de c bits.

Definición de la seguridad pseudo-aleatoria.

Recordemos que $f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c$. Tenemos $T=f(K,M)$, donde T es la etiqueta de c bits determinada por la clave K de c bits y el mensaje M de b bits.

Al adversario A se le presenta un oráculo O que, cuando A le da una pregunta-mensaje, genera una respuesta de c bits. Con probabilidad 50%/50% o (1) el oráculo es $f(K,.)$ con clave aleatoria K, o (2) el oráculo es una función puramente aleatoria.

Definición de la seguridad pseudo-aleatoria.

Recordemos que $f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c$. Tenemos $T=f(K,M)$, donde T es la etiqueta de c bits determinada por la clave K de c bits y el mensaje M de b bits.

Al adversario A se le presenta un oráculo O que, cuando A le da una pregunta-mensaje, genera una respuesta de c bits. Con probabilidad 50%/50% o (1) el oráculo es $f(K,.)$ con clave aleatoria K, o (2) el oráculo es una función puramente aleatoria.

Después de q preguntas, A debe adivinar si O es (1) o (2) con certidumbre >50%,

Definición de la seguridad pseudo-aleatoria.

Recordemos que $f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c$. Tenemos $T=f(K,M)$, donde T es la etiqueta de c bits determinada por la clave K de c bits y el mensaje M de b bits.

Al adversario A se le presenta un oráculo O que, cuando A le da una pregunta-mensaje, genera una respuesta de c bits. Con probabilidad 50%/50% o (1) el oráculo es $f(K,.)$ con clave aleatoria K, o (2) el oráculo es una función puramente aleatoria.

Después de q preguntas, A debe adivinar si O es (1) o (2) con certidumbre >50%, es decir, con probabilidad $\frac{1}{2} + Adv(A)$, donde $Adv(A)$ es la "ventaja de A."

En enero de 2012, Alfred Menezes y yo estábamos pensando sobre el HMAC y comenzando a tener dudas sobre cierto paso crucial en la demostración de Bellare.

En enero de 2012, Alfred Menezes y yo estábamos pensando sobre el HMAC y comenzando a tener dudas sobre cierto paso crucial en la demostración de Bellare.

La demostración de Bellare está escrita en un estilo muy oscuro – sus 12 páginas son sumamente difíciles de leer.

El resumen a continuación es informal y simplificado pero capta la esencia del argumento de Bellare.

En enero de 2012, Alfred Menezes y yo estábamos pensando sobre el HMAC y comenzando a tener dudas sobre cierto paso crucial en la demostración de Bellare.

La demostración de Bellare está escrita en un estilo muy oscuro – sus 12 páginas son sumamente difíciles de leer.

El resumen a continuación es informal y simplificado pero capta la esencia del argumento de Bellare.

En un momento clave de la demostración Bellare describe un adversario de la propiedad pseudo-aleatoria de la función de compresión f que resultaría si HMAC no tuviera la propiedad pseudo-aleatoria deseada.

El fija (M^*, M'^*) igual a un par de mensajes de b bits tal que la probabilidad de un choque $f(K,M^*) = f(K,M'^*)$ (donde la probabilidad es tomada sobre el conjunto de todas las claves K en $\{0,1\}^c$) es máxima.

El fija (M^*, M'^*) igual a un par de mensajes de b bits tal que la probabilidad de un choque $f(K,M^*) = f(K,M'^*)$ (donde la probabilidad es tomada sobre el conjunto de todas las claves K en $\{0,1\}^c$) es máxima.

Usando lo que él llama un argumento "fijando la moneda" (*coin-fixing* en inglés), él incorpora directamente este par de mensajes en su adversario A, quien posteriormente los usará para derrotar la propiedad pseudo-aleatoria de f.

El fija (M^*, M'^*) igual a un par de mensajes de b bits tal que la probabilidad de un choque $f(K,M^*) = f(K,M'^*)$ (donde la probabilidad es tomada sobre el conjunto de todas las claves K en $\{0,1\}^c$) es máxima.

Usando lo que él llama un argumento "fijando la moneda" (*coin-fixing* en inglés), él incorpora directamente este par de mensajes en su adversario A, quien posteriormente los usará para derrotar la propiedad pseudo-aleatoria de f.

Pues este algoritmo A existe en el sentido teórico, ya que el par (M^*, M'^*) obviamente existe.

El fija (M*,M´*) igual a un par de mensajes de b bits tal que la probabilidad de un choque f(K,M*) = f(K,M´*) (donde la probabilidad es tomada sobre el conjunto de todas las claves K en $\{0,1\}^c$) es máxima.

Usando lo que él llama un argumento "fijando la moneda" (*coin-fixing* en inglés), él incorpora directamente este par de mensajes en su adversario A, quien posteriormente los usará para derrotar la propiedad pseudo-aleatoria de f.

Pues este algoritmo A existe en el sentido teórico, ya que el par (M*,M´*) obviamente existe. Pero A es inconstructible en el sentido de que no hay ningún método factible para construirlo.

Las reacciones mias y de Alfred:

Las reacciones mias y de Alfred:

(1)¡Qué barbaridad!

Las reacciones mias y de Alfred:

(1)¡Qué barbaridad!

(2)Los algoritmos son un concepto computacional. En la práctica, ¿qué podría significar un algoritmo que existe matemáticamente pero no es constructible?

Las reacciones mias y de Alfred:

(1)¡Qué barbaridad!

(2)Los algoritmos son un concepto computacional. En la práctica, ¿qué podría significar un algoritmo que existe matemáticamente pero no es constructible?

(3) ¿Qué podríamos decir sobre la seguridad del HMAC en el mundo real si es necesario presuponer que la función de compresión resista hasta los adversarios inconstructibles?

Mihir Bellare es el investigador más citado en toda la criptografía – casi 30 mil referencias en googlescholar.com.

Mihir Bellare es el investigador más citado en toda la criptografía – casi 30 mil referencias en googlescholar.com.

Bellare también es co-inventor (con Rogaway) del concepto de la “seguridad demostrable orientada hacia la práctica,” y la introducción a su trajabo en Crypto 2006 enfatisa la utilidad en el mundo real de sus resultados relacionados a la seguridad del HMAC – un código de autenticación de mensajes usado en todas partes.

Mihir Bellare es el investigador más citado en toda la criptografía – casi 30 mil referencias en googlescholar.com.

Bellare también es co-inventor (con Rogaway) del concepto de la “seguridad demostrable orientada hacia la práctica,” y la introducción a su trajabo en Crypto 2006 enfatisa la utilidad en el mundo real de sus resultados relacionados a la seguridad del HMAC – un código de autenticación de mensajes usado en todas partes. Pareciera sorprendente que tal persona escribiera una demostración de un teorema basada en un argumento dudoso del tipo “fijando la moneda.”

En febrero de 2012 pusimos en el archivo electrónico la primera versión de nuestro artículo “Another Look at HMAC,” el cual explicó el fallo (*flaw*) en el trabajo de Bellare.

En febrero de 2012 pusimos en el archivo electrónico la primera versión de nuestro artículo “Another Look at HMAC,” el cual explicó el fallo (*flaw*) en el trabajo de Bellare.

En unas horas después del puesto del artículo en el archivo, recibimos de Bellare un correo electrónico muy enfadado en que rechazó nuestro uso de la palabra “fallo” y explicó que su demostración es válida en el modelo no uniforme de la complejidad computacional.

En febrero de 2012 pusimos en el archivo electrónico la primera versión de nuestro artículo “Another Look at HMAC,” el cual explicó el fallo (*flaw*) en el trabajo de Bellare.

En unas horas después del puesto del artículo en el archivo, recibimos de Bellare un correo electrónico muy enfadado en que rechazó nuestro uso de la palabra “fallo” y explicó que su demostración es válida en el modelo no uniforme de la complejidad computacional.

En este modelo se permite que un algoritmo tenga una fuente de “consejos” que depende del número de bits en la entrada.

En febrero de 2012 pusimos en el archivo electrónico la primera versión de nuestro artículo “Another Look at HMAC,” el cual explicó el fallo (*flaw*) en el trabajo de Bellare.

En unas horas después del puesto del artículo en el archivo, recibimos de Bellare un correo electrónico muy enfadado en que rechazó nuestro uso de la palabra “fallo” y explicó que su demostración es válida en el modelo no uniforme de la complejidad computacional.

En este modelo se permite que un algoritmo tenga una fuente de “consejos” que depende del número de bits en la entrada. Es decir, un adversario no uniforme podría ser mucho más poderoso que un adversario uniforme.

Le pregunté a Bellare, porque su artículo en ningún lugar no menciona el hecho de que su teorema principal debe ser entendido en el sentido no uniforme y no es válido en el modelo uniforme de la complejidad. Bellare respondió:

Le pregunté a Bellare, porque su artículo en ningún lugar no menciona el hecho de que su teorema principal debe ser entendido en el sentido no uniforme y no es válido en el modelo uniforme de la complejidad. Bellare respondió:

“Mi artículo está escrito dentro del marco de la complejidad concreta, y por eso es intrínsecamente no uniforme…

Le pregunté a Bellare, porque su artículo en ningún lugar no menciona el hecho de que su teorema principal debe ser entendido en el sentido no uniforme y no es válido en el modelo uniforme de la complejidad. Bellare respondió:

“Mi artículo está escrito dentro del marco de la complejidad concreta, y por eso es intrínsecamente no uniforme… nunca me ocurrió que un lector no entendería que cuando la complejidad es concreta tenemos el modelo no uniforme.”

Ahora nos dimos cuenta de que el paso dudoso no fue un lapsus momentáneo por parte de un investigador prominente, sino fue algo permitido en el “modelo no uniforme.”

Ahora nos dimos cuenta de que el paso dudoso no fue un lapsus momentáneo por parte de un investigador prominente, sino fue algo permitido en el “modelo no uniforme.” Bellare justificó su uso del adversario inconstructible, explicando que todo su artículo estuvo escrito en ese modelo de la complejidad computacional.

Ahora nos dimos cuenta de que el paso dudoso no fue un lapsus momentáneo por parte de un investigador prominente, sino fue algo permitido en el "modelo no uniforme." Bellare justificó su uso del adversario inconstructible, explicando que todo su artículo estuvo escrito en ese modelo de la complejidad computacional.

Entonces Alfred y yo examinamos las otras partes del trabajo de Bellare – especialmente su argumento en apoyo de su conclusión de que su teorema justifica el HMAC hasta $2^{c/2}/n$ preguntas – teniendo en mente el modelo no uniforme.

El teorema de Bellare incluye expresiones concretas (es por esta razón que está considerado “orientado hacia la práctica”) que en principio permiten que un ingeniero determine cuántas preguntas del adversario pueden ser soportadas por el HMAC antes de que el teorema ya no garantice nada

El teorema de Bellare incluye expresiones concretas (es por esta razón que está considerado “orientado hacia la práctica”) que en principio permiten que un ingeniero determine cuántas preguntas del adversario pueden ser soportadas por el HMAC antes de que el teorema ya no garantice nada (lo cual ocurre cuando la probabilidad garantizada se vuelva >1).

El teorema de Bellare incluye expresiones concretas (es por esta razón que está considerado “orientado hacia la práctica”) que en principio permiten que un ingeniero determine cuántas preguntas del adversario pueden ser soportadas por el HMAC antes de que el teorema ya no garantice nada (lo cual ocurre cuando la probabilidad garantizada se vuelva >1).

En otras palabras, podemos sustituir los mejores ataques conocidos contra la propiedad pseudo-aleatoria de las funciones de compresión que se usan en el HMAC en el mundo real –

El teorema de Bellare incluye expresiones concretas (es por esta razón que está considerado “orientado hacia la práctica”) que en principio permiten que un ingeniero determine cuántas preguntas del adversario pueden ser soportadas por el HMAC antes de que el teorema ya no garantice nada (lo cual ocurre cuando la probabilidad garantizada se vuelva >1).

En otras palabras, podemos sustituir los mejores ataques conocidos contra la propiedad pseudo-aleatoria de las funciones de compresión que se usan en el HMAC en el mundo real – y es razonable suponer que estas funciones básicas son bien construídas para que los únicos ataques posibles sean los muy generales (ataques “genéricos”) –

El teorema de Bellare incluye expresiones concretas (es por esta razón que está considerado “orientado hacia la práctica”) que en principio permiten que un ingeniero determine cuántas preguntas del adversario pueden ser soportadas por el HMAC antes de que el teorema ya no garantice nada (lo cual ocurre cuando la probabilidad garantizada se vuelva >1).

En otras palabras, podemos sustituir los mejores ataques conocidos contra la propiedad pseudo-aleatoria de las funciones de compresión que se usan en el HMAC en el mundo real – y es razonable suponer que estas funciones básicas son bien construídas para que los únicos ataques posibles sean los muy generales (ataques “genéricos”) – y hallar los límites impuestos sobre los parámetros para que el teorema de Bellare no pierda su contenido.

Esto es lo que hace Bellare en su trabajo en Crypto 2006 en su interpretación de su teorema.

Esto es lo que hace Bellare en su trabajo en Crypto 2006 en su interpretación de su teorema.

El supone que el mejor ataque conocido contra la propiedad pseudo-aleatoria de f es búsqueda exhaustiva de la clave.

Esto es lo que hace Bellare en su trabajo en Crypto 2006 en su interpretación de su teorema.

El supone que el mejor ataque conocido contra la propiedad pseudo-aleatoria de f es búsqueda exhaustiva de la clave. En este caso el adversario tiene ventaja de aproximadamente 2^{-c}.

Esto es lo que hace Bellare en su trabajo en Crypto 2006 en su interpretación de su teorema.

El supone que el mejor ataque conocido contra la propiedad pseudo-aleatoria de f es búsqueda exhaustiva de la clave. En este caso el adversario tiene ventaja de aproximadamente 2^{-c}.

En el sentido clásico (uniforme) de un algoritmo esta presuposición es completamente razonable, ya que nadie conoce nada mejor.

Esto es lo que hace Bellare en su trabajo en Crypto 2006 en su interpretación de su teorema.

El supone que el mejor ataque conocido contra la propiedad pseudo-aleatoria de f es búsqueda exhaustiva de la clave. En este caso el adversario tiene ventaja de aproximadamente 2^{-c}.

En el sentido clásico (uniforme) de un algoritmo esta presuposición es completamente razonable, ya que nadie conoce nada mejor.

Pero recordemos que Bellare insistió que está trabajando en el modelo no uniforme de la complejidad, y que cualquier estudio concreto de la seguridad debe ser cumplido en este modelo (y que nunca le había ocurrido que alguien pudiera no entender eso).

Prontamente Alfred y yo encontramos que la presuposición de Bellare es completamente falsa en el modelo no uniforme.

Prontamente Alfred y yo encontramos que la presuposición de Bellare es completamente falsa en el modelo no uniforme.

De hecho, es muy fácil demostrar eso.

Prontamente Alfred y yo encontramos que la presuposición de Bellare es completamente falsa en el modelo no uniforme.

De hecho, es muy fácil demostrar eso.

Se puede describir un adversario inconstructible muy sencillo pero muy poderoso contra la propiedad pseudo-aleatoria de f,

Prontamente Alfred y yo encontramos que la presuposición de Bellare es completamente falsa en el modelo no uniforme.

De hecho, es muy fácil demostrar eso.

Se puede describir un adversario inconstructible muy sencillo pero muy poderoso contra la propiedad pseudo-aleatoria de f, lo cual resulta en que el número de bits de seguridad en la garantía de Bellare debe ser reducido por más de la mitad – de 60 a 28 cuando c=160 y de 44 a 20 cuando c=128.

Prontamente Alfred y yo encontramos que la presuposición de Bellare es completamente falsa en el modelo no uniforme.

De hecho, es muy fácil demostrar eso.

Se puede describir un adversario inconstructible muy sencillo pero muy poderoso contra la propiedad pseudo-aleatoria de f, lo cual resulta en que el número de bits de seguridad en la garantía de Bellare debe ser reducido por más de la mitad – de 60 a 28 cuando c=160 y de 44 a 20 cuando c=128.

En la práctica 28 o 20 bits de seguridad no tienen valor alguno.

Prontamente Alfred y yo encontramos que la presuposición de Bellare es completamente falsa en el modelo no uniforme.

De hecho, es muy fácil demostrar eso.

Se puede describir un adversario inconstructible muy sencillo pero muy poderoso contra la propiedad pseudo-aleatoria de f, lo cual resulta en que el número de bits de seguridad en la garantía de Bellare debe ser reducido por más de la mitad – de 60 a 28 cuando c=160 y de 44 a 20 cuando c=128.

En la práctica 28 o 20 bits de seguridad no tienen valor alguno.

Para explicar este adversario muy poderoso, voy a pedir la ayuda del Mono de Fútbol.

El Mono de Fútbol es un amigo cercano del "mono con una máquina de escribir," quien con una cantidad suficiente de tiempo puede aleatoriamente escribir *Macbeth* sin error alguno, pero en la práctica no va a lograr escribir nada más que "Entran tres brujas…".

El Mono de Fútbol no comparte con su amigo el deseo de escribir copias perfectas de las obras grandes de la literatura.

El Mono de Fútbol no comparte con su amigo el deseo de escribir copias perfectas de las obras grandes de la literatura.

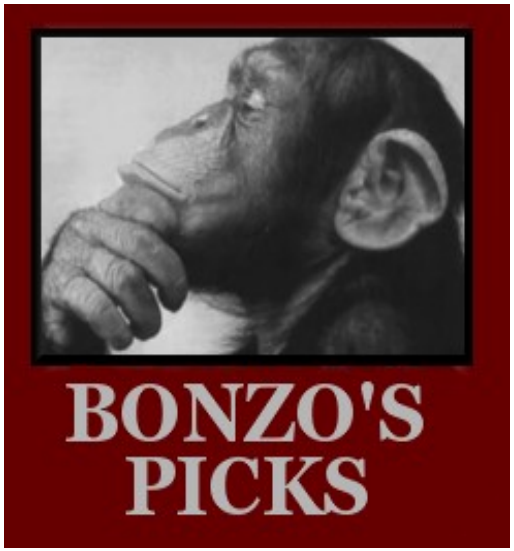
Más bien, todas las semanas durante la temporada del fútbol norteamericano el Mono proclama sus “selecciones” para la semana – quienes van a ganar.

El Mono de Fútbol no comparte con su amigo el deseo de escribir copias perfectas de las obras grandes de la literatura.

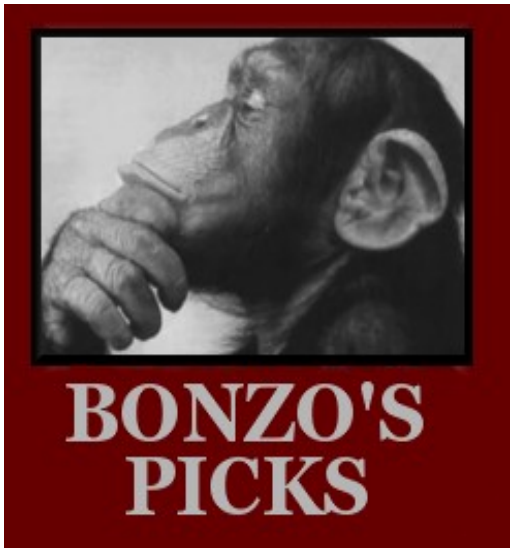
Más bien, todas las semanas durante la temporada del fútbol norteamericano el Mono proclama sus "selecciones" para la semana – quienes van a ganar.

De la misma manera de un comentador humano de fútbol, el Mono está muy contento y orgulloso cada vez que tiene resultado mejor del 50% / 50%.

El ataque del Mono contra la propiedad pseudo-aleatoria de la NFL (liga de fútbol nacional de los Estados Unidos).

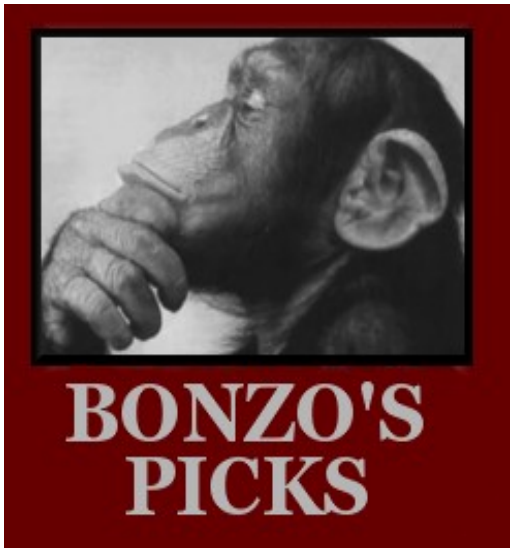


El ataque del Mono contra la propiedad pseudo-aleatoria de la NFL (liga de fútbol nacional de los Estados Unidos).



Supongamos que la temporada consiste en 256 partidos (eso no es exacto).

El ataque del Mono contra la propiedad pseudo-aleatoria de la NFL (liga de fútbol nacional de los Estados Unidos).



Supongamos que la temporada consiste en 256 partidos (eso no es exacto). En este ataque el Mono logrará seleccionar los equipos ganadores con éxito: 144/112 correctos/incorrectos en vez de 128/128.

A continuación sigue el ataque no uniforme:

A continuación sigue el ataque no uniforme:

TOMA LA MEJOR TEMPORADA DEL MONO!

A continuación sigue el ataque no uniforme:

TOMA LA MEJOR TEMPORADA DEL MONO!

Según la teoría de los paseos aleatorios, la desviación estandar de 128/128 va a ser $2^{c/2}$ donde $2^{c} = 256$, es decir, 16.

A continuación sigue el ataque no uniforme:

TOMA LA MEJOR TEMPORADA DEL MONO!

Según la teoría de los paseos aleatorios, la desviación estandar de 128/128 va a ser $2^{c/2}$ donde $2^{c} = 256$, es decir, 16.

Puede ser que el Mono tiene el resultado 112/144 en vez de 144/112,

A continuación sigue el ataque no uniforme:

TOMA LA MEJOR TEMPORADA DEL MONO!

Según la teoría de los paseos aleatorios, la desviación estandar de 128/128 va a ser $2^{c/2}$ donde $2^{c} = 256$, es decir, 16.

Puede ser que el Mono tiene el resultado 112/144 en vez de 144/112, pero nuestro adversario puede tomar su mejor temporada, por lo cual este adversario tiene una ventaja significativa.

Por favor no cedan a la tentación de decir
“¡Todo eso es trivial y estúpido!”

Por favor no cedan a la tentación de decir
“¡Todo eso es trivial y estúpido!”

Realmente, el ataque del Mono de Fútbol es el método usado por Alfred y mí para demostrar que el teorema principal del trabajo de Bellare en Crypto 2006
que trata sobre la seguridad del HMAC carece de valor alguno en la práctica.

Por favor no cedan a la tentación de decir
“¡Todo eso es trivial y estúpido!”

Realmente, el ataque del Mono de Fútbol es el método usado por Alfred y mí para demostrar que el teorema principal del trabajo de Bellare en Crypto 2006
que trata sobre la seguridad del HMAC carece de valor alguno en la práctica.

Es decir, el Mono puede ser usado para crear un adversario genérico contra la propiedad pseudo-aleatoria cuya ventaja es mucho, mucho mayor de la ventaja de la búsqueda exhaustiva.

Para cualquier subconjunto S de {1,2,…,c}, cualquier mensaje M en $\{0,1\}^b$ y cualquier bit t, definamos la función $u_{S,M,t}(K)$ para K variable en $\{0,1\}^c$ como:

Para cualquier subconjunto S de {1,2,…,c}, cualquier mensaje M en $\{0,1\}^b$ y cualquier bit t, definamos la función $u_{S,M,t}(K)$ para K variable en $\{0,1\}^c$ como:

1, si la suma-XOR de los bits de f(K,M) con índices en S es igual a t; 0, si es igual a 1-t.

Para cualquier subconjunto S de {1,2,…,c}, cualquier mensaje M en $\{0,1\}^b$ y cualquier bit t, definamos la función $u_{S,M,t}(K)$ para K variable en $\{0,1\}^c$ como:

1, si la suma-XOR de los bits de f(K,M) con índices en S es igual a t; 0, si es igual a 1-t.

Pongamos (S*,M*,t*) igual a un triple fijo tal que la probabilidad (tomada sobre el conjunto de todas las claves K) de que $u_{S^*,M^*,t^*}(K)=1$ es máxima.

Para cualquier subconjunto S de {1,2,…,c}, cualquier mensaje M en $\{0,1\}^b$ y cualquier bit t, definamos la función $u_{S,M,t}(K)$ para K variable en $\{0,1\}^c$ como:

1, si la suma-XOR de los bits de f(K,M) con índices en S es igual a t; 0, si es igual a 1-t.

Pongamos (S*,M*,t*) igual a un triple fijo tal que la probabilidad (tomada sobre el conjunto de todas las claves K) de que $u_{S^*,M^*,t^*}(K)=1$ es máxima.

La selección del triple (S*,M*,t*) en su esencia es la misma cosa que la selección de la mejor temporada del Mono de Fútbol en el caso cuando el Mono de Fútbol fue el adversario de la propiedad pseudo-aleatoria de la secuencia de ganadoras de los partidos de la NFL.

Nuestro adversario A tiene el triple (S*,M*,t*) incorporado directamente en su memoria.

Nuestro adversario A tiene el triple (S*,M*,t*) incorporado directamente en su memoria.

El necesita nada más que una pregunta — el mensaje M* — y el oráculo responde O(M*).

Nuestro adversario A tiene el triple (S*,M*,t*) incorporado directamente en su memoria.

El necesita nada más que una pregunta — el mensaje M* — y el oráculo responde O(M*).

Si la suma-XOR de los bits de O(M*) con índices en S* es igual a t*, entonces A adivina que O realmente es f(K,.);

Nuestro adversario A tiene el triple (S*,M*,t*) incorporado directamente en su memoria.

El necesita nada más que una pregunta — el mensaje M* — y el oráculo responde O(M*).

Si la suma-XOR de los bits de O(M*) con índices en S* es igual a t*, entonces A adivina que O realmente es f(K,.);

si es igual a 1-t*, entonces A adivina que O es una función aleatoria.

Usando la desviación estandar de un paseo aleatorio, facilmente encontramos que la ventaja esperada de A es $\geq 2^{-c/2}$.

Usando la desviación estandar de un paseo aleatorio, facilmente encontramos que la ventaja esperada de A es $\geq 2^{-c/2}$. (Usando el hecho de que la ventaja de A fue maximizada sobre un conjunto de 2^{b+c+1} triples, podemos mejorar un poco esta desigualdad:

$$Adv(A) \geq (b+c)^{1/2}\, 2^{-c/2}.\ )$$

Usando la desviación estandar de un paseo aleatorio, facilmente encontramos que la ventaja esperada de A es $\geq 2^{-c/2}$. (Usando el hecho de que la ventaja de A fue maximizada sobre un conjunto de 2^{b+c+1} triples, podemos mejorar un poco esta desigualdad:

$$Adv(A) \geq (b+c)^{1/2}\, 2^{-c/2}.)$$

Nuestro adversario A es mucho más poderoso que la búsqueda exhaustiva, la cual tiene ventaja solamente $\approx 2^{-c}$.

Usando la desviación estandar de un paseo aleatorio, facilmente encontramos que la ventaja esperada de A es $\geq 2^{-c/2}$. (Usando el hecho de que la ventaja de A fue maximizada sobre un conjunto de 2^{b+c+1} triples, podemos mejorar un poco esta desigualdad:

$$Adv(A) \geq (b+c)^{1/2}\, 2^{-c/2}.\ )$$

Nuestro adversario A es mucho más poderoso que la búsqueda exhaustiva, la cual tiene ventaja solamente $\approx 2^{-c}$.

Las funciones "típicas" (tales como las funciones de compresión que se usan en la práctica) no van a poder resistir este adversario no uniforme A. Entonces, podemos considerar que A es un adversario genérico.

Las consecuencias para la interpretación práctica del teorema principal de Bellare son catastróficas.

Las consecuencias para la interpretación práctica del teorema principal de Bellare son catastróficas.

En vez de justificar el HMAC hasta 2^{44} o 2^{60} preguntas para las dos formas del HMAC más comunes (el HMAC-MD5 y el HMAC-SHA1), resulta del adversario de Mono de Fútbol:

Las consecuencias para la interpretación práctica del teorema principal de Bellare son catastróficas.

En vez de justificar el HMAC hasta 2^{44} o 2^{60} preguntas para las dos formas del HMAC más comunes (el HMAC-MD5 y el HMAC-SHA1), resulta del adversario de Mono de Fútbol: ¡su teorema carece de contenido alguno después de 2^{20} preguntas para HMAC-MD5 y 2^{28} para HMAC-SHA1!

Las consecuencias para la interpretación práctica del teorema principal de Bellare son catastróficas.

En vez de justificar el HMAC hasta 2^{44} o 2^{60} preguntas para las dos formas del HMAC más comunes (el HMAC-MD5 y el HMAC-SHA1), resulta del adversario de Mono de Fútbol: ¡su teorema carece de contenido alguno después de 2^{20} preguntas para HMAC-MD5 y 2^{28} para HMAC-SHA1!

Se puede concluir que la simulación de la seguridad de datos a través del "modelo no uniforme" de la complejidad computacional (o sea, a través de los adversarios inconstructibles) ha funcionado muy mal.

Referencia: “Another Look at HMAC” y “Another Look at Non-Uniformity,” http://anotherlook.ca

Nuestra serie de trabajos contiene muchas críticas de la simulación matemática en la criptografía.

Referencia: “Another Look at HMAC” y “Another Look at Non-Uniformity,” http://anotherlook.ca

Nuestra serie de trabajos contiene muchas críticas de la simulación matemática en la criptografía. El objetivo principal de este sitio web es explicar las limitaciones de las demostraciones matemáticas en cuestiones de la seguridad de datos.

Referencia: “Another Look at HMAC” y “Another Look at Non-Uniformity,” http://anotherlook.ca

Nuestra serie de trabajos contiene muchas críticas de la simulación matemática en la criptografía. El objetivo principal de este sitio web es explicar las limitaciones de las demostraciones matemáticas en cuestiones de la seguridad de datos.

Los ejemplos del fracaso en el uso de la simulación matemática incluyen los ataques del tipo “selección de claves para firma duplicada” y el teorema de Bellare sobre la seguridad del HMAC.

Otra situación en que la simulación no ha funcionado bien: los ataques “por canales laterales.”

Otra situación en que la simulación no ha funcionado bien: los ataques “por canales laterales.”

En estos ataques el adversario recolecta medidas de: los tiempos para la ejecución de varios pasos, la emisión de la radiación, el uso de la energía, los resultados de ciertos fallos inducidos, etcétera.

Otra situación en que la simulación no ha funcionado bien: los ataques “por canales laterales.”

En estos ataques el adversario recolecta medidas de: los tiempos para la ejecución de varios pasos, la emisión de la radiación, el uso de la energía, los resultados de ciertos fallos inducidos, etcétera.

Por ejemplo, el método común (“elevar al cuadrado y multiplicar”) para elevar a la potencia de un número entero binario requiere más tiempo (y más energía) cada vez que tiene el bit 1 que requiere cuando tiene el bit 0.

Otra situación en que la simulación no ha funcionado bien: los ataques “por canales laterales.”

En estos ataques el adversario recolecta medidas de: los tiempos para la ejecución de varios pasos, la emisión de la radiación, el uso de la energía, los resultados de ciertos fallos inducidos, etcétera.

Por ejemplo, el método común (“elevar al cuadrado y multiplicar”) para elevar a la potencia de un número entero binario requiere más tiempo (y más energía) cada vez que tiene el bit 1 que requiere cuando tiene el bit 0.

A veces un ataque por canal lateral puede determinar todos los bits de una clave secreta.

En muchos campos — la economía, la criptografía, y otros — los investigadores tienden a poner mucha fé en los métodos matemáticos. ¿Porqué?

En muchos campos — la economía, la criptografía, y otros — los investigadores tienden a poner mucha fé en los métodos matemáticos. ¿Porqué?

Las matemáticas — tanto las matemáticas puras como aplicadas — tienen la reputación de ser el mejor modelo del pensamiento riguroso e imparcial.

En muchos campos — la economía, la criptografía, y otros — los investigadores tienden a poner mucha fé en los métodos matemáticos. ¿Porqué?

Las matemáticas — tanto las matemáticas puras como aplicadas — tienen la reputación de ser el mejor modelo del pensamiento riguroso e imparcial.

Por esta razón en muchos países el público tiene confianza completa en el uso de los exámenes de matemáticas para seleccionar a los estudiantes para admisión a las universidades más prestigiosas.

En muchos campos — la economía, la criptografía, y otros — los investigadores tienden a poner mucha fé en los métodos matemáticos. ¿Porqué?

Las matemáticas — tanto las matemáticas puras como aplicadas — tienen la reputación de ser el mejor modelo del pensamiento riguroso e imparcial.

Por esta razón en muchos países el público tiene confianza completa en el uso de los exámenes de matemáticas para seleccionar a los estudiantes para admisión a las universidades más prestigiosas.

Esta característica del pensamiento matemático es también la justificación principal para enseñarlas a todos los futuros ciudadanos, no solamente a los que van a usar las matemáticas en su trabajo.

En los Estados Unidos los estudiantes que quieren proseguir una carrera de abogado tienen más posibilidad de inscribirse en un buen programa de posgrado en jurisprudencia si han recibido buenas calificaciones en las asignaturas de matemáticas que en las de “ciencia política.”

En los Estados Unidos los estudiantes que quieren proseguir una carrera de abogado tienen más posibilidad de inscribirse en un buen programa de posgrado en jurisprudencia si han recibido buenas calificaciones en las asignaturas de matemáticas que en las de “ciencia política.” El comité de admisión va a entender que en el primer caso los estudiantes han desarrollado los hábitos del pensamiento riguroso, mientras que en el segundo caso todo lo contrario.

En los Estados Unidos los estudiantes que quieren proseguir una carrera de abogado tienen más posibilidad de inscribirse en un buen programa de posgrado en jurisprudencia si han recibido buenas calificaciones en las asignaturas de matemáticas que en las de “ciencia política.” El comité de admisión va a entender que en el primer caso los estudiantes han desarrollado los hábitos del pensamiento riguroso, mientras que en el segundo caso todo lo contrario.

Otro ejemplo:
CETI = Comunicación con Inteligencia Extraterrestre.

En los Estados Unidos los estudiantes que quieren proseguir una carrera de abogado tienen más posibilidad de inscribirse en un buen programa de posgrado en jurisprudencia si han recibido buenas calificaciones en las asignaturas de matemáticas que en las de “ciencia política.” El comité de admisión va a entender que en el primer caso los estudiantes han desarrollado los hábitos del pensamiento riguroso, mientras que en el segundo caso todo lo contrario.

Otro ejemplo:
CETI = Comunicación con Inteligencia Extraterrestre.
En este trabajo se han desarrollado lenguajes matemáticos para cualquier futura necesidad de comunicación con criaturas inteligentes que vienen de otros planetas.

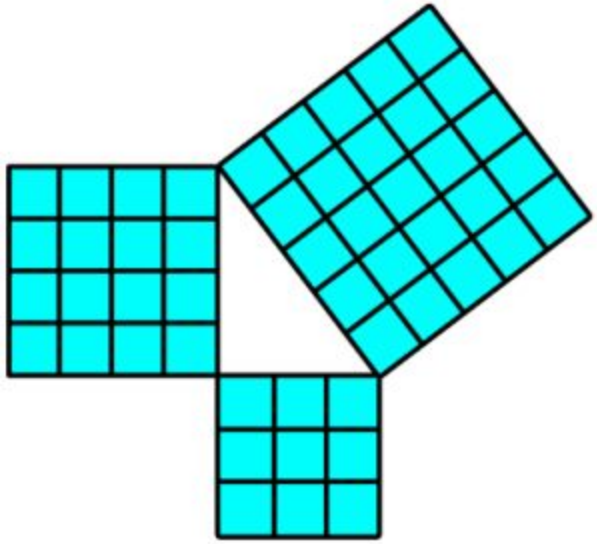
¿Porqué las matemáticas?

¿Porqué las matemáticas?

Porque son el único lenguaje universal.

¿Porqué las matemáticas?

Porque son el único lenguaje universal.



Es probable que esta imagen se entienda por cualquier criatura inteligente en cualquier parte del universo.

Igualmente la secuencia de números