



Criptografía cuántica Detección de intrusos



OWASP

The Open Web Application Security Project

About Me



OWASP

The Open Web Application Security Project

- Jose Dante Cortez Guachalla
 - Informática – Ingeniería de Sistemas UMSA
 - MDeTEL Miguel de Cervantes – España
 - CISO (Oficial de Seguridad)
 - MTA (Microsoft Technologi Associate)
 - Especialidad en derecho Informatico



OWASP

The Open Web Application Security Project

- Contenido

- Definiciones

- Física clásica, física cuántica
 - Criptografía

- Estructura física y lógica

- Modelo de criptografía cuántica

- Detección de intrusos

- Aplicabilidad del modelo

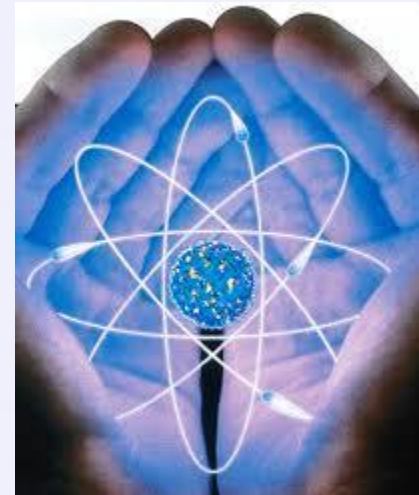
Definiciones



OWASP

The Open Web Application Security Project

- ¿Qué distingue a la física mecánica de la física cuántica?



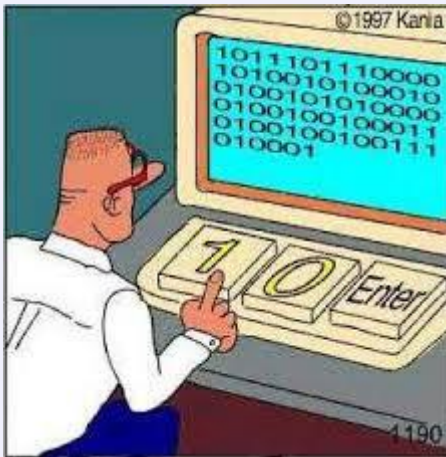
Definiciones







OWASP

The Open Web Application Security Project

- Bit



Qbit

	
Polarizacion Vertical	Polarizacion Horizontal
	
Polarizacion diagonal derecha	Polrizacion diagonal izquierda

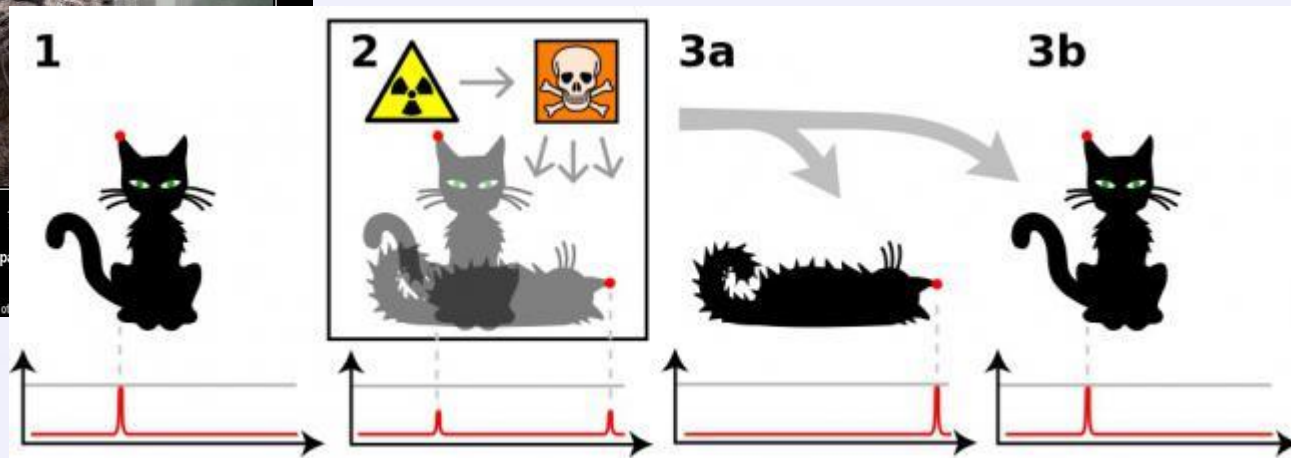
Definiciones



OWASP

The Open Web Application Security Project

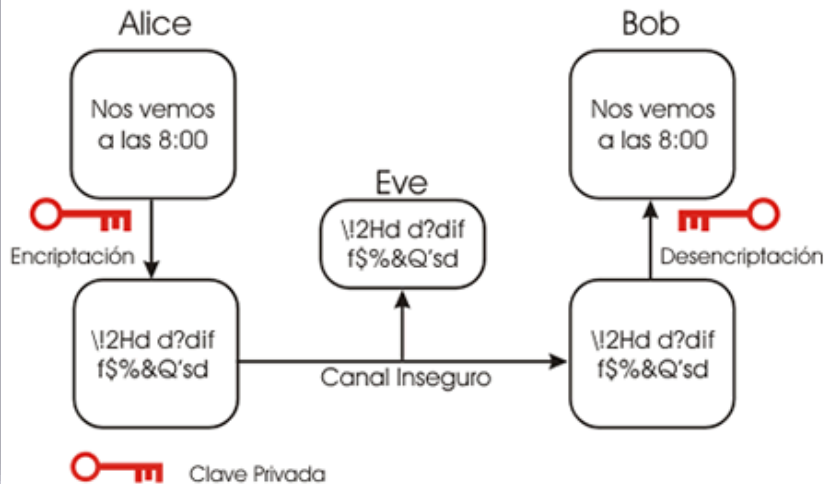
- Gato de shchinder



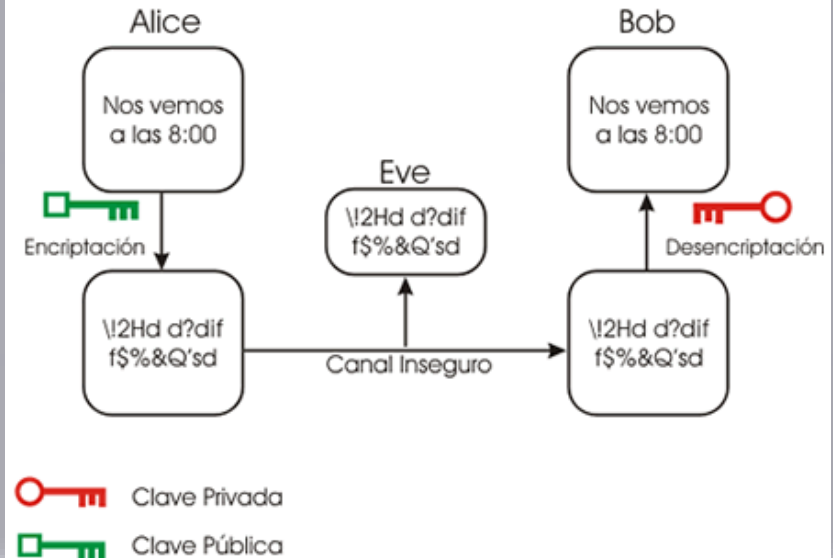


- Criptografía

Criptografía de Clave Privada



Criptografía de Clave Pública

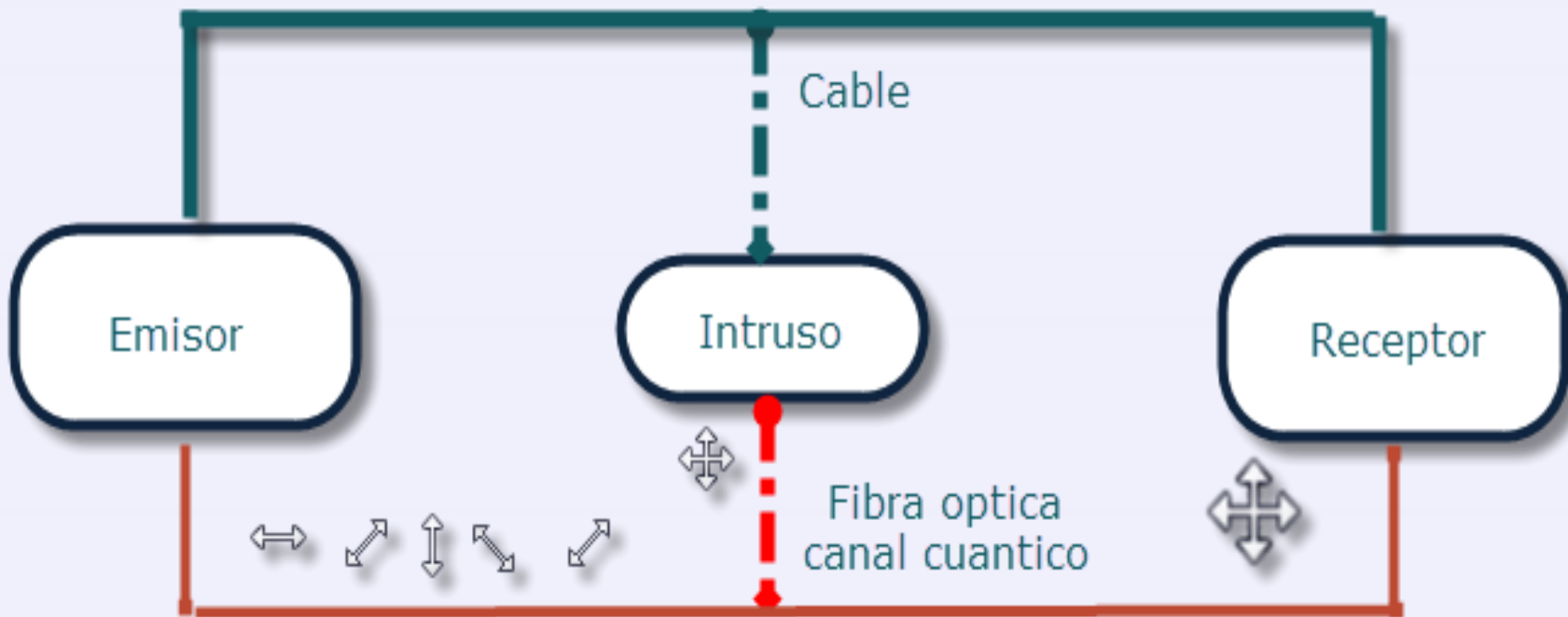


Modelo criptográfico cuántico



OWASP

The Open Web Application Security Project



Detección de intrusos



OWASP

The Open Web Application Security Project

Los 25 fotones están distribuidos de la siguiente manera:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

En presencia del atacante, el intruso intercepta los fotones polarizados, eligiendo al azar el filtro para cada uno de los fotones, además con el supuesto de que el intruso capturó la secuencia que establece el lenguaje para los 25 fotones

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Por cada interceptación de lectura, existe la probabilidad del 0.3 (30%) de que el detector falle su lectura:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Detección de intrusos



OWASP

The Open Web Application Security Project

La probabilidad de que el detector falle, también es del 30%

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Después del intercambio de información a través del canal cuántico, el receptor envía por un canal público los fotones que fueron detectados con éxito, el emisor responde por el mismo canal, validando todos los datos que fueron enviados

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Detección de intrusos



OWASP

The Open Web Application Security Project

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

El emisor realiza el análisis de los datos aceptados como aciertos, por parte del receptor, y evidencia que la probabilidad de no lectura de los detectores de fotones es de 0.3, de un total de 25 datos enviados, la tolerancia a fallo es de 7,5 fotones sin detectar.

Envío aceptado mayor o igual al N° qubits * $P(f)$, es decir

N° qubits = 25

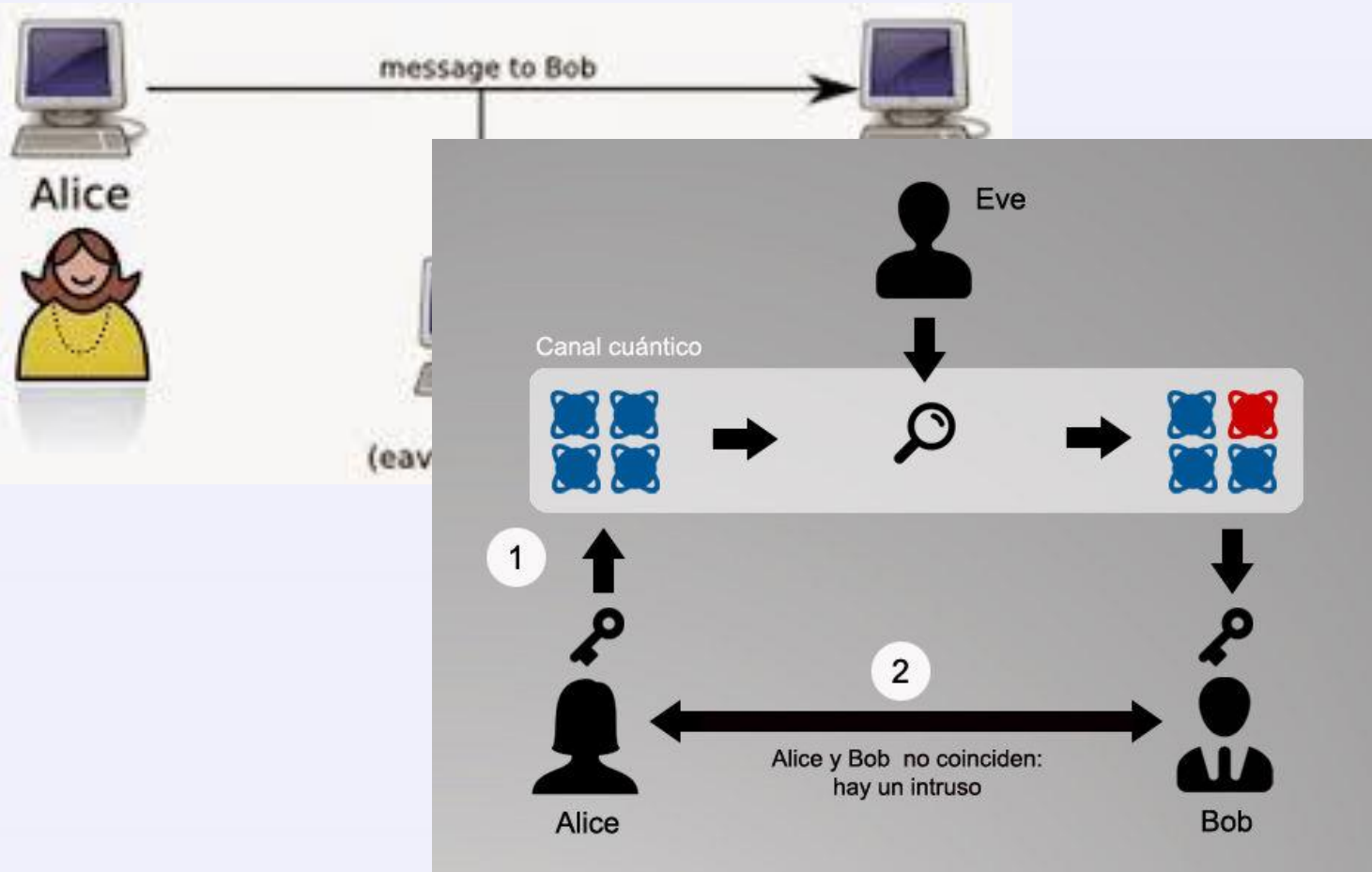
$P(f) = 0.3$; probabilidad de no detección del lector

En este caso especial se trata de:

Envío aceptado debe ser mayor o igual a $= 25 * 0.3 = 7.5$

La cantidad de aciertos es igual a 6, por lo que se evidencia la presencia de un intruso, escuchando los datos que son enviados, por lo que el emisor reinicia el sistema y vuelve a realizar el procedimiento de autenticación.

Detección de intrusos





OWASP

The Open Web Application Security Project

- **Gracias !!!**