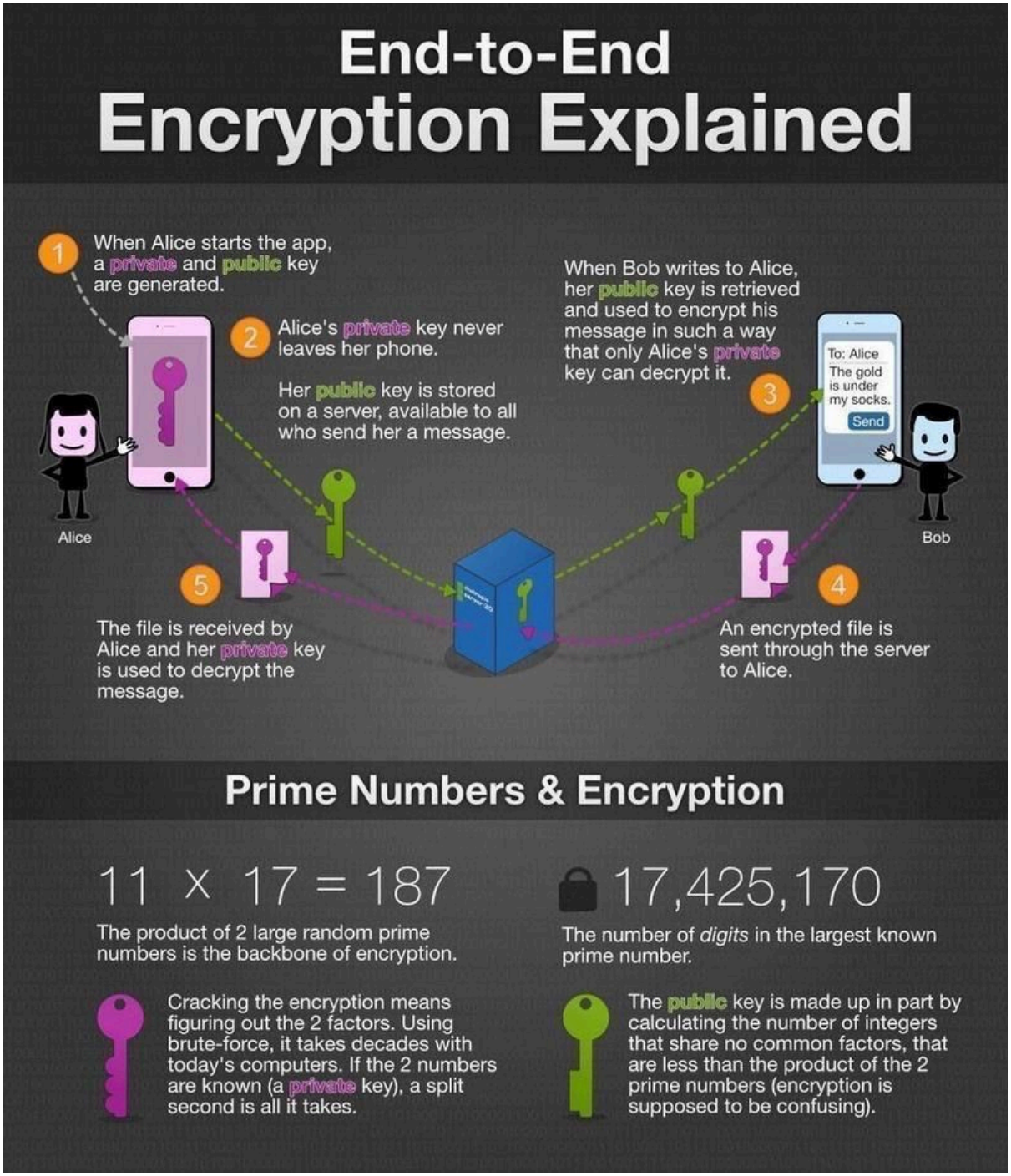
Universidad de Buenos Aires
Facultad de Ciencias Económicas

Encriptación de Extremo a Extremo

Material de Estudio



Traducción y Comentarios

CIFRADO DE EXTREMO A EXTREMO (END-TO-END ENCRYPTION – E2EE)

Qué significa Cifrado de Extremo a Extremo

El **Cifrado de Extremo a Extremo** (*End-to-End Encryption – E2EE*) es un mecanismo de seguridad mediante el cual **solo el emisor y el receptor de un mensaje pueden leer su contenido**.

Ni los servidores intermedios, ni el proveedor del servicio, ni terceros pueden acceder al mensaje en texto legible.

Desde la perspectiva de los **Sistemas de Información**, el E2EE es un componente crítico para la **confidencialidad de la información**, la protección de datos sensibles y el cumplimiento normativo.

Cómo funciona el cifrado de extremo a extremo (paso a paso)

1. Generación de claves

Cuando una usuaria inicia una aplicación segura:

- Se generan dos claves:
  - **Clave pública (Public Key)**
  - **Clave privada (Private Key)**

Estas claves forman parte de un sistema de **criptografía asimétrica** (*Asymmetric Cryptography*).

---

2. Protección de la clave privada

- La **clave privada** nunca sale del dispositivo del usuario.
- Permanece almacenada localmente y es conocida únicamente por su propietario.

Desde la gestión de TI, esto implica que **ni siquiera el proveedor del sistema puede descifrar los mensajes**.

---

3. Uso de la clave pública

- La **clave pública** se almacena en un servidor.
- Está disponible para cualquier persona que desee enviar un mensaje cifrado.

Cuando un remitente envía un mensaje:

- Recupera la clave pública del destinatario.
- Cifra el mensaje utilizando esa clave pública.

---

4. Envío del mensaje cifrado

- El mensaje cifrado viaja a través de servidores y redes.
- Aunque sea interceptado, **no puede ser leído**, ya que está en formato cifrado.

Esto demuestra que la seguridad **no depende del canal**, sino del cifrado.

---

5. Descifrado del mensaje

- El destinatario recibe el mensaje cifrado.
- Utiliza su **clave privada** para descifrarlo.
- El mensaje vuelve a su forma original y legible.

Solo quien posee la clave privada puede realizar este proceso.

Relación entre números primos y cifrado (Prime Numbers & Encryption)

Fundamento matemático

La criptografía moderna se basa en **números primos grandes** (*Prime Numbers*).

Ejemplo simple:

- 11 × 17 = 187

Multiplicar es fácil.

Descubrir los factores originales sin conocerlos previamente es **mucho más complejo** cuando los números son extremadamente grandes.

Por qué es seguro

- El cifrado se apoya en el hecho de que **factorizar números primos enormes requiere décadas de cálculo**, incluso con computadoras modernas.
- Si se conocen los factores (equivalente a conocer la **clave privada**), el descifrado es inmediato.
- Si no se conocen, el proceso es computacionalmente inviable.

Claves y complejidad

- La **clave pública** se construye usando cálculos matemáticos complejos basados en números primos.
- La **clave privada** contiene la información crítica necesaria para revertir el proceso.
- La seguridad se basa en la **asimetría del esfuerzo computacional**: cifrar es fácil, descifrar sin la clave es prácticamente imposible.

Implicancias para la administración y los sistemas de información

Confidencialidad de la información

El E2EE protege:

- Comunicaciones corporativas
- Datos financieros
- Información estratégica
- Datos personales de clientes y empleados

Gestión del riesgo

- Reduce el riesgo de fuga de información.
- Limita el impacto de ataques a servidores centrales.
- Traslada la responsabilidad de la seguridad criptográfica al diseño del sistema.

Cumplimiento normativo

El cifrado de extremo a extremo contribuye al cumplimiento de:

- Normativas de protección de datos
- Requisitos de confidencialidad
- Buenas prácticas de seguridad de la información

Limitaciones organizacionales

- Si un usuario pierde su clave privada, **la información no puede recuperarse**.
- No existe una "puerta trasera" sin comprometer la seguridad del sistema.
- La administración debe contemplar políticas claras de respaldo, gestión de dispositivos y continuidad operativa.

Idea central a retener

El cifrado de extremo a extremo **no protege los servidores, protege la información**.

La seguridad no depende de la confianza en el proveedor, sino de principios matemáticos sólidos y del correcto diseño de los sistemas de información.

Para la administración moderna, comprender este mecanismo es esencial para **tomar decisiones informadas sobre tecnología, riesgo, costos y responsabilidad organizacional**.

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.