XI Congreso Internacional de Investigación y Práctica Profesional en Psicología. XXVI Jornadas de Investigación. XV Encuentro de Investigadores en Psicología del MERCOSUR. I Encuentro de Investigación de Terapia Ocupacional. I Encuentro de Musicoterapia. Facultad de Psicología - Universidad de Buenos Aires, Buenos Aires, 2019.

Aportes de la criptología al campo psicoanalítico.

Jofre, Alan.

APORTES DE LA CRIPTOLOGÍA AL CAMPO PSICOANALÍTICO

Jofre, Alan
Universidad de Buenos Aires. Facultad de Psicología. Argentina

RESUMEN
Se introducirán teóricamente las funciones de la criptología, disciplina que comprende tanto las técnicas criptográficas (de cifrado) como las criptoanalíticas (de desciframiento), en su interés para el psicoanálisis. Para dicha tarea, será necesario transmitir una introducción básica a los conceptos centrales de la criptología, que implica un análisis de los principales componentes de los criptosistemas.

Palabras clave
Criptografía - Criptoanálisis - Criptología - Psicoanálisis

ABSTRACT
CONTRIBUTIONS OF CRYPTOLOGY TO THE PSYCHOANALYTIC FIELD
The contributions of cryptology to the psychoanalytic field will be introduced theoretically, including both cryptographic (encryption) and cryptanalytic (deciphering) techniques. For this task, it will be necessary to begin with a basic introduction to the main concepts of cryptology which also involves an analysis of the main components of cryptosystems.

Key words
Cryptography - Cryptanalysis - Psychoanalysis - Cryptology

Introducción: El síntoma como mensaje cifrado.

"Cada cual es definido en cada momento, y hasta en su actitud sexual, por el hecho de que una carta siempre llega a destino" (Lacan, 1954, 307)

Antes de poder realizar una articulación conceptual entre el psicoanálisis y la criptología es necesario la incorporación de algunas nociones básicas. Presentaré entonces el esquema básico que fundamenta un acto de cifrado, o sea una operación criptográfica. Podemos afirmar que el fundamento de una operación de cifrado es proteger un mensaje y en su función más básica la criptografía supone los medios que posibilitan entregar un mensaje de forma protegida frente a un "adversario". (Bellare, Phillip Rogaway, 2005). En este sentido, un sistema criptográfico puede ser visualizado como esquema de la comunicación "Emisor - Receptor" de Shannon al que se le incorpora otra entidad, llamada convencionalmente como Adversario. Lo podemos graficar del siguiente modo:

Esquema de comunicación insegura

E > *m1* > R
^
Ad

Un emisor "E" tiene que entregar un mensaje "*m1*" a un receptor "R" frente al riesgo de que un adversario "Ad" intercepte el mensaje, comprometiendo la seguridad de la comunicación. Como podemos ver que este esquema es inseguro ya que el Adversario consigue el mensaje que está siendo transmitido, "*m1"*. El hecho de que se pretenda que el mensaje sea protegido de la lectura de un adversario justifica la necesidad de la encriptación o cifrado, y para eso es necesario que haya algún tipo de sistema criptográfico o criptosistema. Un criptosistema en su mínima expresión entonces implica un algoritmo "A" de cifrado y descifrado, una llave determinada y un mensaje a encriptar.

Esquema simétrico de comunicación segura

E {*m1*}.A > *m2* >R {*m2*}.A > *m*1
^
Ad

Ahora bien, este esquema es algo más complicado. Partiendo de un mensaje sin cifrar, que denomino "*m1"* y una llave "{ }" o clave, el emisor "E" encripta "*m1"* a través de un algoritmo "A" convirtiéndolo en "*m2"* o mensaje cifrado. El "*m2"* protege el mensaje ante un posible Adversario "Ad" que pueda interceptarlo en alguna parte de su recorrido. Es importante notar entonces que "Ad" se encuentra con un mensaje cifrado y no con "*m1"*. Eventualmente, "R" utiliza la misma llave que se usó en la encriptación en "A" y con "*m2"* para recuperar el contenido que había sido cifrado, es decir, hacer legible "*m1"*. Se produce un desciframiento, inversamente a cómo se produjo un cifrado. Un criptoanálisis es el reverso de esta operación, consiste entonces en las técnicas usadas para "romper" un encriptamiento, volviendo el mensaje cifrado legible. Se habla de ruptura de un encriptamiento o un cifrado, es decir de un criptoanálisis cuando no se posee una clave de desciframiento, sino directamente se iniciaría el proceso de descifrado. La operación criptoanalítica es por lo tanto propia del lugar de Adversario.

Esquema de operación criptoanalítica

Ad = *m2*.{?}.A > *m*1

La operación criptoanalítica se da entonces en el nivel de operación del Adversario, porque el mismo parte de un mensaje cifrado y no sabe la llave de desciframiento (Goldreich, 2003). Según el principio de Kerckhoffs aunque todo el criptosistema sea conocido, puede mantenerse seguro si se desconoce la llave (Diffie y Hellman, 1976). Con este principio también se relaciona la máxima de Shannon que afirma "El enemigo conoce el sistema" (Shannon, 1949). Sin este plus de saber que es la llave que el Adversario no posee, no se puede desencriptar el mensaje cifrado y por lo tanto de hace necesaria la operación criptoanalítica y por otra parte se puede conocer el algoritmo sin que se vea comprometida la seguridad del criptosistema de ninguna manera.

Criptoanálisis y criptoestructura

En textos como "*La Interpretación de Los Sueños*" (Freud, 1900), "*Psicopatología de la vida cotidiana*" (Freud, 1901) o "*El Chiste y su relación con lo Inconciente*" (Freud, 1905) y en verdad en la mayoría de los textos de la primer tópica freudiana podemos encontrar intentos de abordaje de Freud de problemáticas que están claramente dentro del espectro de la criptología, tanto en la elucidación de los procesos de cifrado que implican los fenómenos psíquicos con que trabaja, como en los desarrollos técnicos que apuntan a un intento de desciframiento.

En el capítulo dos de "*La interpretación de los sueños*" aclara que una técnica científica de interpretación de los sueños no consiste en traducir los elementos del sueño con una clave fija, como en los *Traumbuch*, o libros de sueños. De aquí que su técnica de interpretación se encuentre más cerca del *Chiffriermethode* o método de desciframiento (Freud, 1900) Pero se debe aclarar que aquí usa la palabra *Chiffrier* en un sentido vulgar y no criptológico. El sueño no responde a una codificación sino a un cifrado.

Por su parte se puede leer en el Seminario dos de Lacan: "El término clave de la cibernética es *mensaje.* El lenguaje está hecho para eso, pero no se trata de un código, es esencialmente ambiguo (...) Por su parte, la frase posee un sentido único, quiero decir que no puede lexicalizarse: se hacen diccionarios de palabras, de empleo de las palabras o de las locuciones, pero no se hacen diccionarios de frases." (Lacan, 1954, 413).

El cifrado o encriptación en un sentido clásico es la transformación de una cadena de texto (texto pleno) de un estado en legible a otro que impide su lectura, protegiendo su contenido. Siguiendo esta misma dirección podemos considerar que una cadena de significantes puede cifrarse y que por lo tanto se transforma en otro u otros significantes. Este es el problema con que se encuentra Freud en la clínica de las neurosis desde que realiza un primer abordaje del síntoma. Desde esta perspectiva se puede afirmar que en su trabajo clínico Freud, operando desde el lugar del adversario tal y como lo entiende la criptología, intercepta un "*m*2" que él infiere que responde a un "*m*1" que fue procesado a través de determinados mecanismos: en última instancia desplazamientos y condensaciones. La criptografía clásica, es decir la que se desarrolla hasta el nacimiento de la computación y los nuevos paradigmas de encriptación, se resume precisamente en dos mecanismos homologables a los mencionados freudianos: transposición y sustitución. En última instancia, operaciones sobre una cadena.

Por este motivo podemos afirmar que Freud realizaba una operación criptoanalítica propiamente dicha en este movimiento de desciframiento, un intento de ruptura de las distintas formaciones del inconciente que él toma como *textos cifrados*: el síntoma, el sueño, los lapsus, etc. Tal vez uno de los casos más paradigmáticos sea el que Freud aborda primeramente en "Sobre el mecanismo psíquico de la desmemoria" *Signorelli*, donde realiza una descomposición de los procesos de cifrado que producen los significantes "*Boticcelli" y "Boltraffio"* (Freud, 1898).

Efectivamente se puede operar criptoanalíticamente, produciendo rupturas y desciframientos a partir de las formaciones del inconciente, por lo tanto podemos considerar que el inconciente mismo es un sistema criptográfico o un criptosistema tal como lo entiende la criptología. Propongo denominarlo entonces criptoestructura, dado que la naturaleza de este criptosistema en particular corresponde a la estructura del significante.

En su análisis del chiste *famillonario*, Lacan se pregunta lo siguiente: "¿Qué nos dice Freud? Que reconocemos aquí el mecanismo de la condensación, materializada en el material del significante, se trata de una especie de encastrado, con ayuda de no sé qué máquina, de dos líneas de la cadena significante". Se puede considerar que la máquina a la que hace alusión Lacan no está por fuera del significante en sí mismo: La letra "A" de los esquemas criptográficos desarrollados al principio de este trabajo corresponde al Otro. Puede considerarse entonces al Otro como un algoritmo de cifrado y descifrado, una maquinaria significante en constante producción y sanción de materiales encriptados.

Algunas conclusiones

Cada formación del inconciente está estructurada criptográficamente en tanto hay una encriptación que no responde a un código, sino a una operatoria de transposición y sustitución. Conocer las implicancias de las problemáticas de la criptología para el campo psicoanalítico es imprescindible para reformular algunos interrogantes de la teoría y práctica psicoanalítica. El aporte que puede hacer esta disciplina es por lo tanto inestimable, tanto en la consideración del síntoma como de toda la estructura que lo produce como tal.

Dado que desde una perspectiva psicoanalítica las formaciones del inconciente son producto de un cifrado dentro de la lógica significante, considero a las operaciones de desciframiento efectuadas por Freud y posteriormente por Lacan como criptoanalíticas. Propongo denominarlas en su especifidad y con una finalidad pragmática como operaciones *criptopsicoanalíticas*.

Por otra parte, al revisar los aportes de la criptología encontra-

mos el fundamento de la magnitud de la tarea de desciframiento que conlleva un psicoanálisis. Una tarea de desciframiento supera en varios órdenes de magnitud el tiempo y el trabajo que implica un cifrado. Por el principio de Kerckhoffs inferimos que no basta con conocer el criptosistema para producir un desciframiento: es necesario tener una llave. Llamo a esta llave *plus de saber.*

Por este motivo, el psicoanálisis no se basa exclusivamente en conocer la criptoestructura con la que trabaja, sino que en la práctica se requiere poseer una llave de desciframiento que siempre es singular y significante: elemento que sólo la clínica contempla. Sobre esta base podemos diferenciar estrictamente la psicología de la del psicoanálisis.

Excede los fines de este trabajo realizar un desarrollo exhaustivo de las ramas o los desarrollos actuales de la criptología, pero su interés para el psicoanálisis no se agota en los desarrollos clásicos de esta disciplina, sino que también puede enriquecerse de los paradigmas criptográficos contemporáneos: deben ser objeto de próximas investigaciones.

BIBLIOGRAFÍA

Bellare, M. y Rogaway, P. (2005). "*Introduction to Modern Cryptography"*.

Diffie, W., y Hellman, M. (1976, Noviembre). "New Directions in Cryptography." *IEEE Transactions on information theory*, *it-22*(6), 644-654.

Freud, S. (1900). "*Sobre el mecanismo psíquico de la desmemoria"*. Buenos Aires: Amorrortu, 1991.

Freud, S. (1900). "*La interpretación de los Sueños"*. Buenos Aires: Amorrortu, 1991.

Freud, S. (1901). "*Psicopatología de la vida cotidiana (Sobre el olvido, los deslices en el habla, el trastrocar las cosas confundido, la superstición y el error)"*. Buenos Aires: Amorrortu, 1991.

Freud, S. (1905). "*El Chiste y su relación con lo Inconciente"*. Buenos Aires: Amorrortu, 1991.

Goldreich, O. (2003). "*Foundations of Cryptography: Basic Tools."* Cambridge: Cambridge University Press.

Lacan, J. (1954). *Seminario 2: "El yo en la teoría de Freud y en la técnica psicoanálitica".* Buenos Aires: Paidós, 2008.

Lacan, J. (1957). *Seminario 5: "Las formaciones del inconciente".* Buenos Aires: Paidós, 1999.

Shannon, C. (1949, Octubre). "Communication Theory of Secrecy Systems". *Bell System Technical Journal.* (28). Recuperado 2 de Mayo 2019.