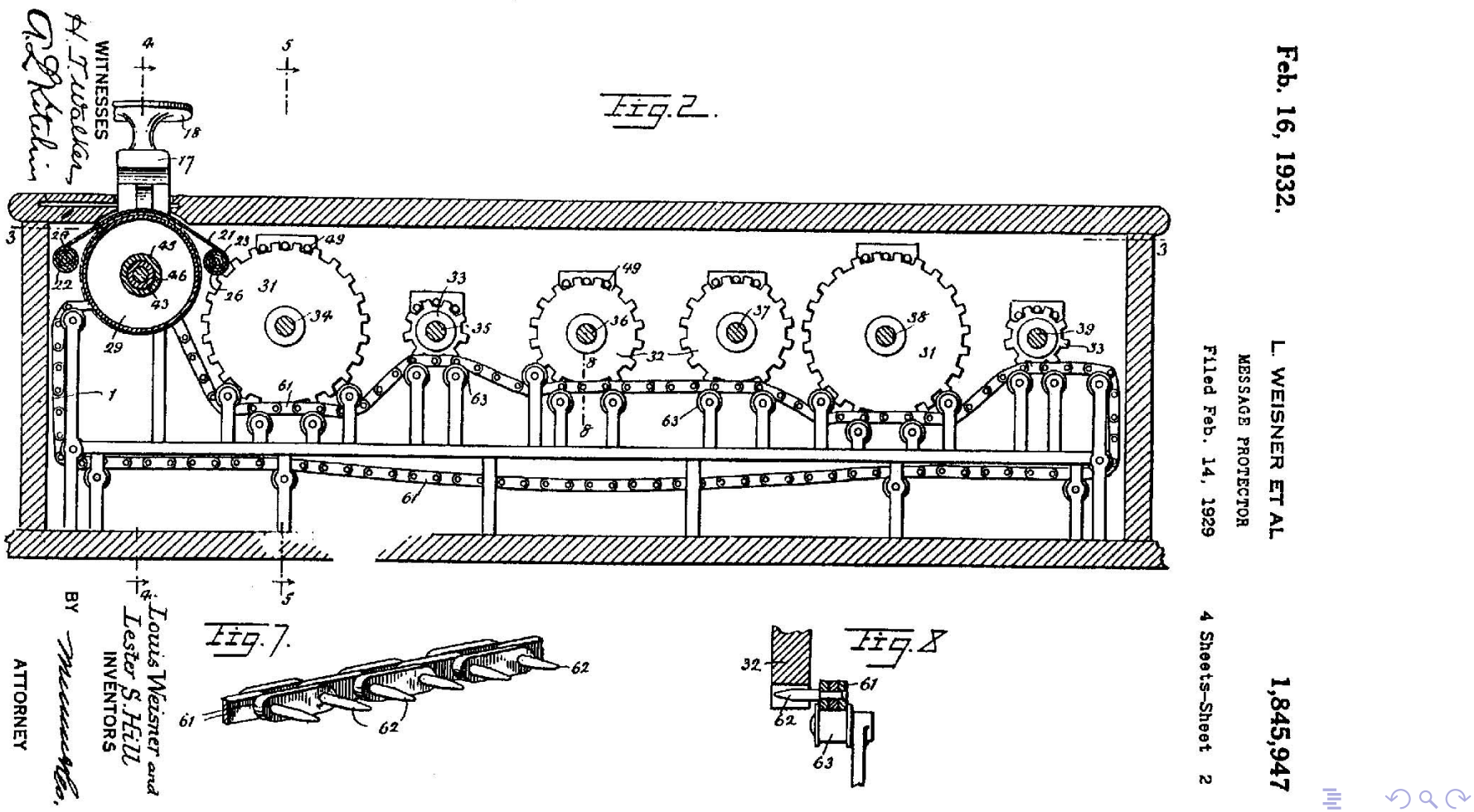
Mechanical Message Protector

- Louis Weisner & Lester Hill
- U.S. patent number 1845947 from 1929



Hill Cipher

- Linear Transformation of the digitized alphabet
- A.[uncoded message] $=$ [coded message]

$$A \begin{bmatrix} \text{col1=start of message} & \dots & \text{coln=end of message} \end{bmatrix}$$

- Mechanical device: 6×6 matrix
- Method is vulnerable to those that intercept enough vector correspondances (uncoded and coded) because of its linearity.
- Final project idea: linear methods of cracking the cipher
- More powerful computers - RSA cryptosystem

1929 Hill's Message Protector

1946 ENIAC

1965 TI four-function calculator

1976 TI-30

1977 Tex

1978 RSA Cryptosystem

1981 IBM 5150 PC

1982 Maple 1.0

1984 MATLAB, Mac Desktop

1985 Casio Graphing Calc.

1985 LaTex, Microsoft Excel

1988 Mathematica 1.0

1991 SMART Board

1996 TI-83