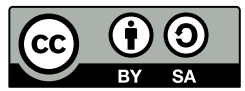
Privacy and Security in Health Information

Saulius Gražulis

Vilnius, 2024

Vilnius University Institute of Biotechnology

Id: slides.tex 1524 2020-06-04 11:58:32Z saulius May 27, 2024



Encryption systems

- Symmetric ciphers

$$C = E_K(M)$$

$$M = E_K(C)$$

- Public key ciphers

$$C = E_{K_{\text{Public}}}(M)$$

$$M = E_{K_{\text{Private}}}(C)$$

Uses of encryption systems

- Secret communication:

$$C = E_{K_{\text{Public}}}(M)$$

$$M = E_{K_{\text{Private}}}(C)$$

- Digital signatures:

$$S = E_{K_{\text{Private}}}(M)$$

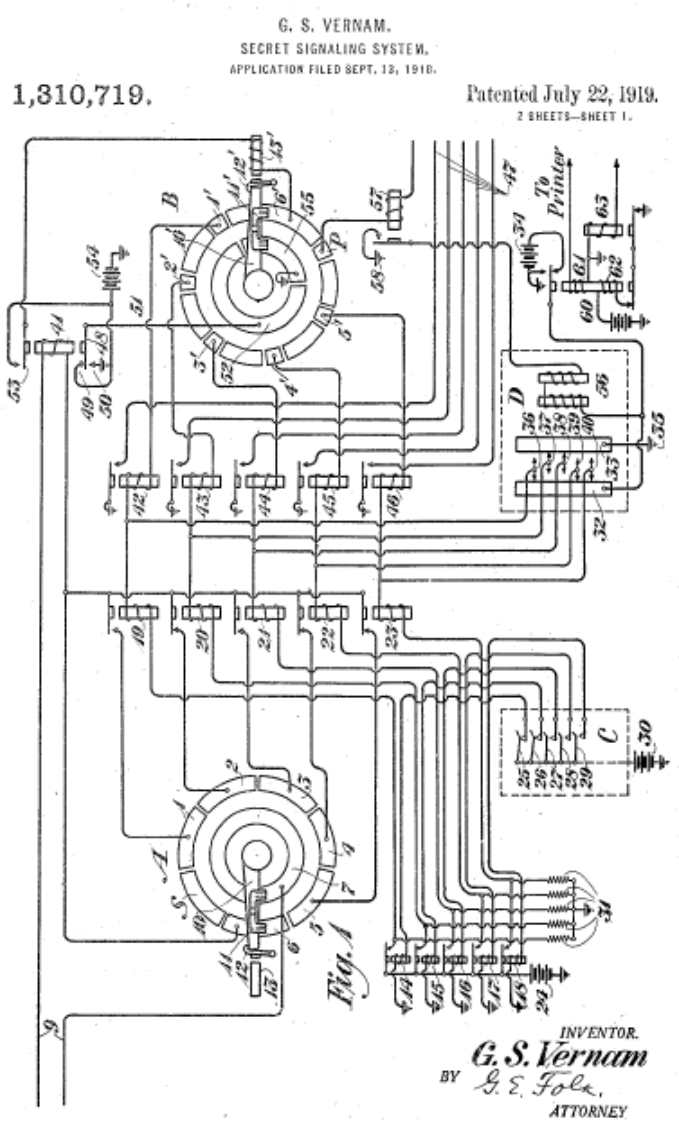
$$M = E_{K_{\text{Public}}}(S)$$

- Authentication

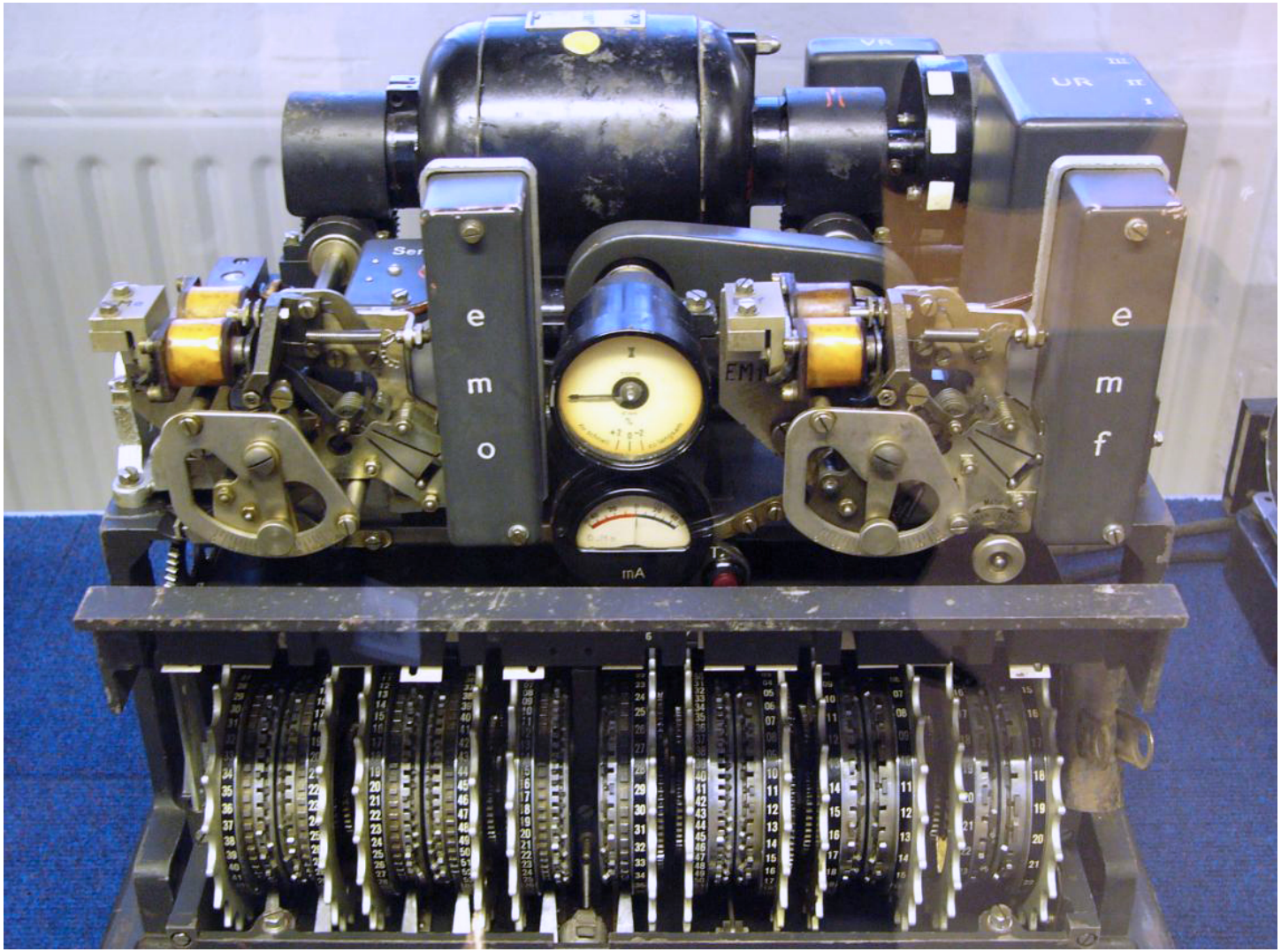
$$\text{Response} = E_{K_{\text{Private}}}(\mathit{Challenge})$$

Example: Vernam cipher

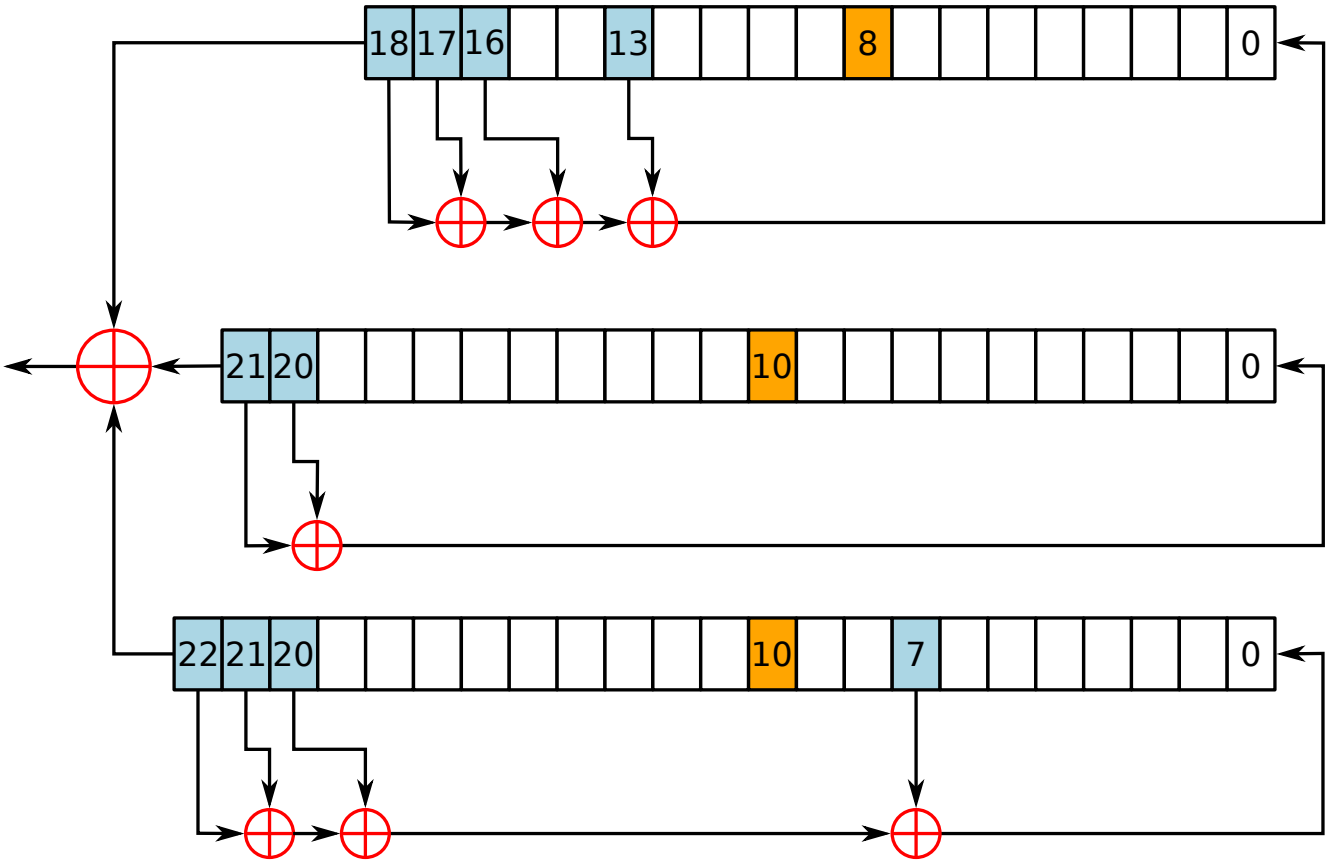
A	B	$A \oplus B$
0	0	0
1	0	1
0	1	1
1	1	0



Example: Lorenz cipher



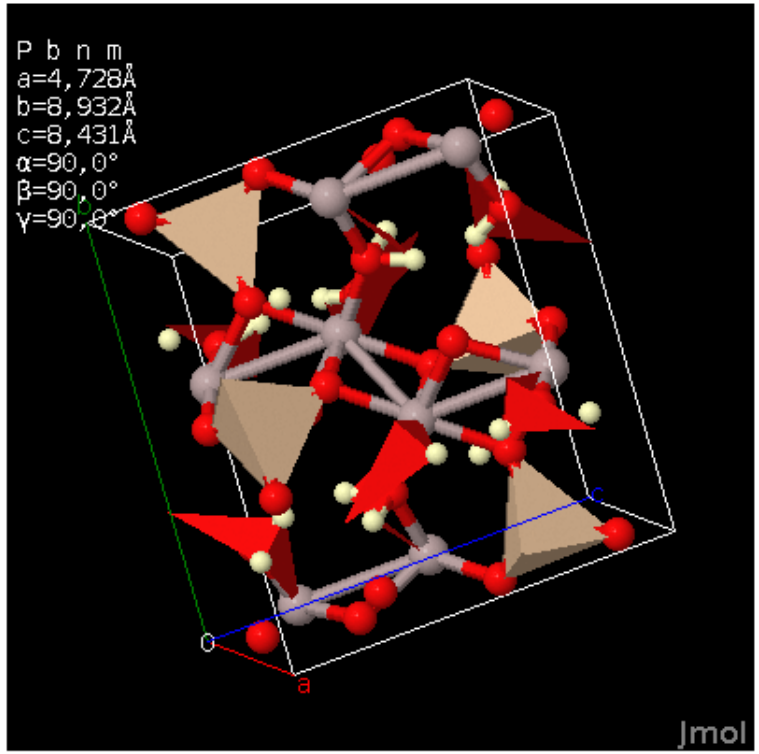
Example: GSM cipher



ssh

- `ssh-keygen` – generate a new key;
- `ssh-keygen -l -f key` – list the key fingerprint;
- `ssh` – secure shell;
- `scp` – secure copy;
- `ssh-add` – add a key;
- `ssh-add -l` – list available keys;

Thank you!



Coordinates	2207377.cif
Original IUCr paper	HTML

http://en.wikipedia.org/wiki/Topaz

http://www.crystallography.net/2207377.html

References I