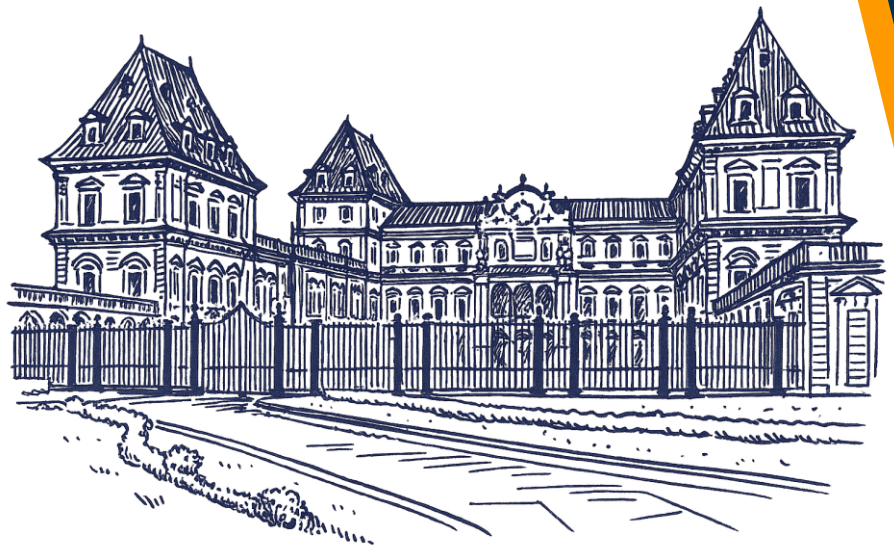
An aperitif on modern cryptography

Leonardo Errati



Politecnico di Torino | CrypTO

1. Against entropy...

Atbash cipher

*“And after all of them, the king of **Sheshak** will drink it too.”*

(Book of Jeremiah, 25:26)

Sheshak

shin-shin-kaf

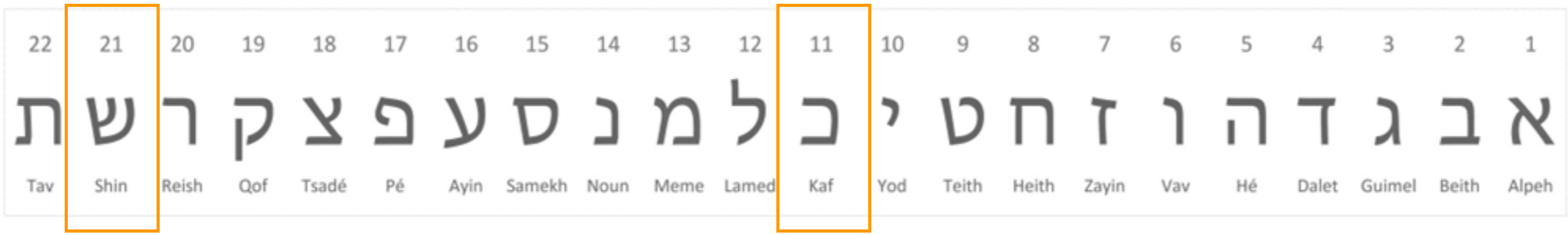
Atbash cipher

*"And after all of them, the king of **Sheshak** will drink it too."*

(Book of Jeremiah, 25:26)

Sheshak

shin-shin-kaf $\xrightarrow{\varphi_{atbash}}$ *bet-bet-lamed*



$$\varphi_{atbash}\colon \mathbb{Z}_{22} \to \mathbb{Z}_{22}$$
$$x \mapsto (23 - x)\ mod\ 22$$

A ⟶ Z
B ⟶ Y
C ⟶ X

Atbash cipher

*"And after all of them, the king of **Sheshak** will drink it too."*

(Book of Jeremiah, 25:26)

Sheshak

shin-shin-kaf

φ_{atbash}

Babylon

bet-bet-lamed

$$\varphi_{atbash}\colon \mathbb{Z}_{22} \to \mathbb{Z}_{22}$$
$$x \mapsto (23 - x)\ mod\ 22$$

A ⟶ Z
B ⟶ Y
C ⟶ X

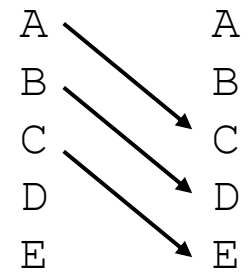
Caesar cipher

$$\varphi_{caesar}\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \mapsto (x + k)\ mod\ 26$$

```
message:      ATTACKATDAWN
key:          C
ciphertext:   DWWDFNDWGDZQ
```

$$H(K) = -\sum_{k \in K} P[k] \cdot \log_2 P[k]$$

$$H_{caesar} \simeq 4.7$$



Vigenere cipher

$$k = (k_0, \dots, k_{t-1})$$

$$\varphi_{vigenere}: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \mapsto (x_i + k_{i \bmod t}) \bmod 26$$

```
message:      ATTACKATDAWN
key:          keykeykeykey
ciphertext:   KXRKGIKXBYAL
```

$$H_{vigenere} \simeq 4.7 \cdot t$$

Vigenere cipher

$$k = (k_0, \dots, k_{t-1})$$

$$\varphi_{vigenere}: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \mapsto (x_i + k_{i \bmod t}) \bmod 26$$

```
message:      ATTACKATDAWN
key:          keykeykeykey
ciphertext:   KXRKGIKXBKAL
```

$$H_{vigenere} \simeq 4.7 \cdot t$$

Vernam cipher

$$k = (k_0, \dots, k_{n-1})$$

$$\varphi_{vernam}: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x_i \mapsto (x_i + k_{i \bmod n}) \bmod 26$$

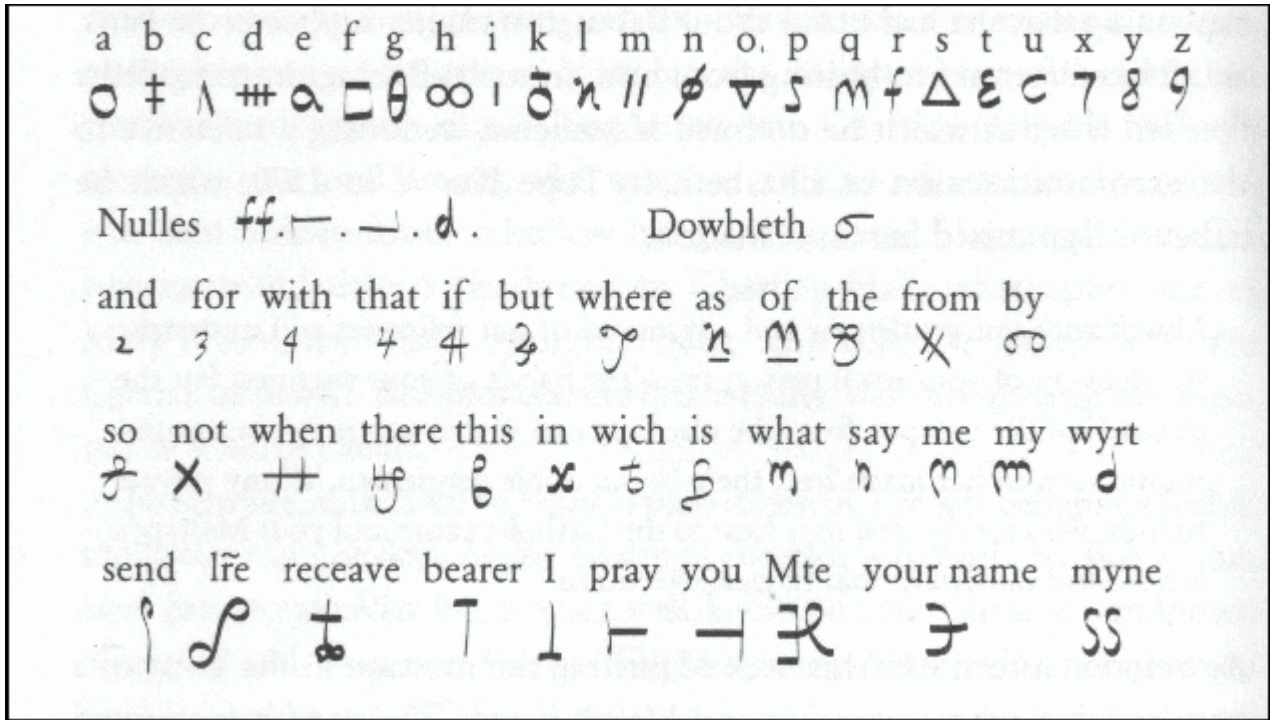
```
message:      ATTACKATDAWN
key:          aezklwgrmali
ciphertext:   AXSKNGGKPOHV
```

$$H_{vernam} \simeq 4.7 \cdot n$$

If k is uniformly distributed and independent on m this cipher is perfect, i.e.

$$P[M = m \,|C = c] = P[M = m]$$

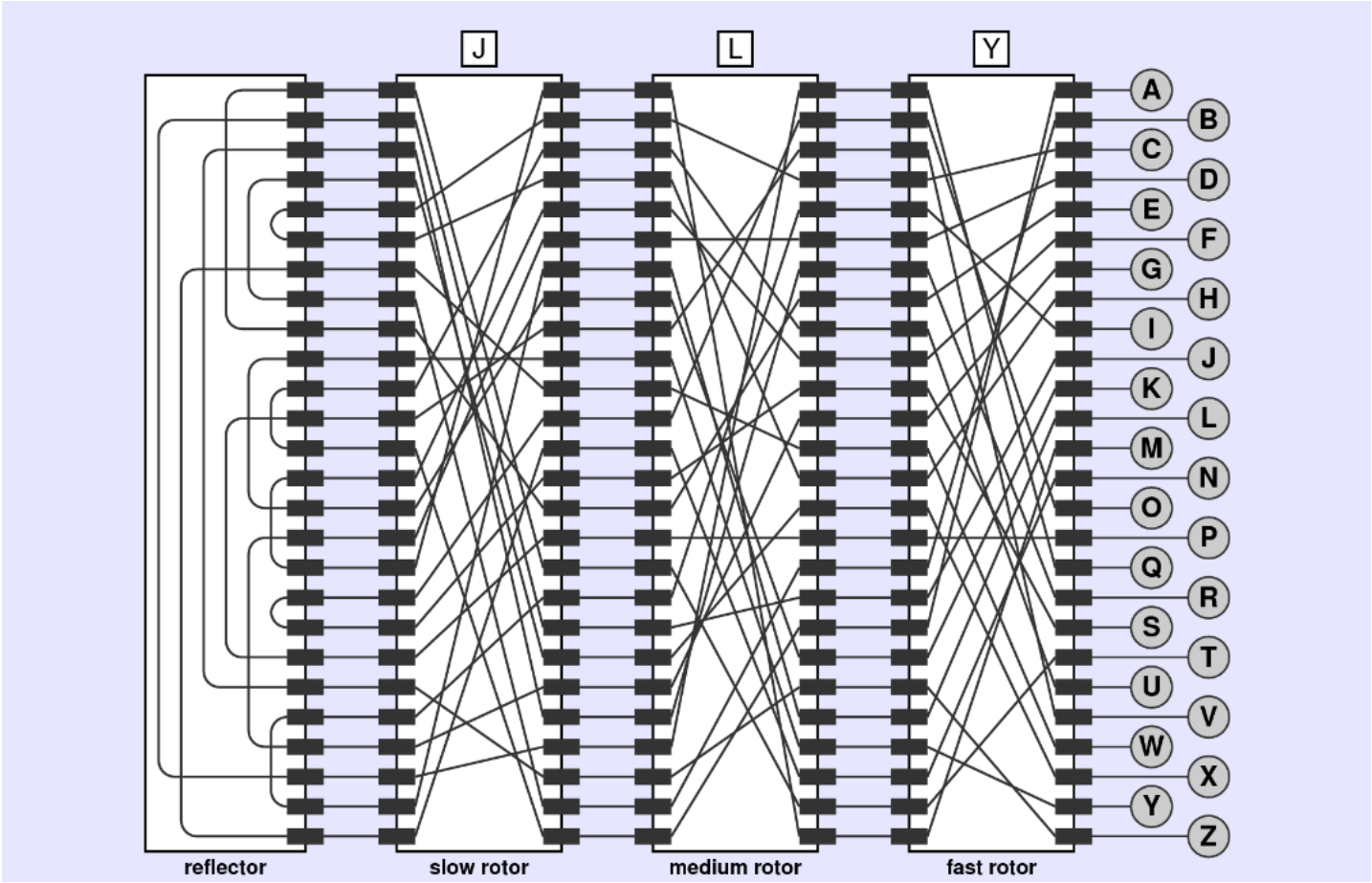
Nomenclators



1. Against entropy...
2. Machines themselves...

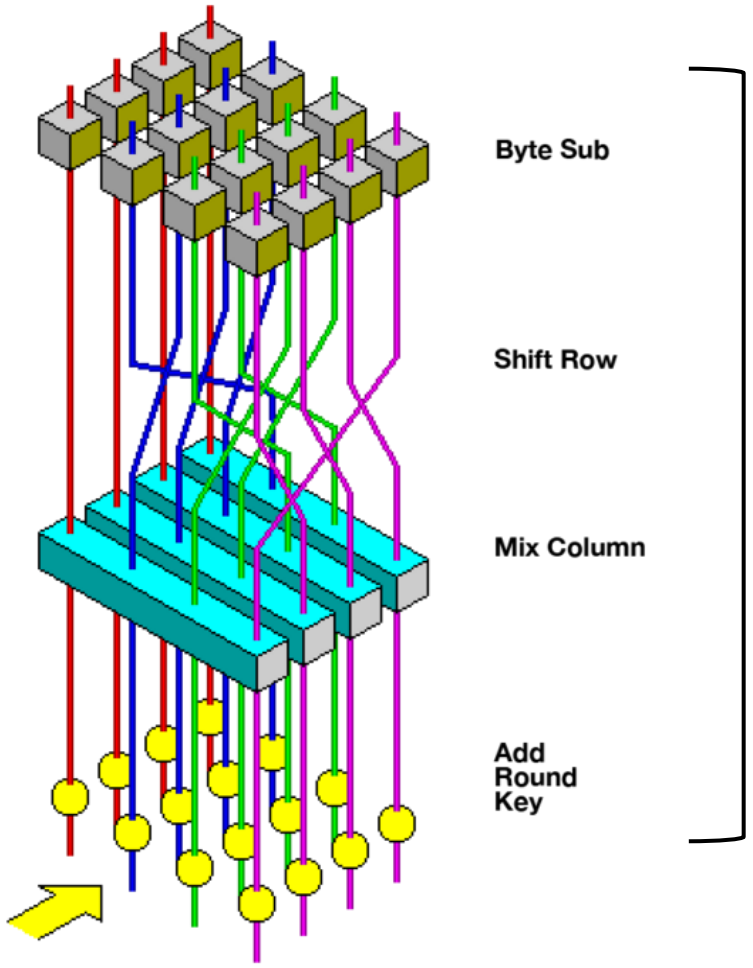
Diskret cipher machine

Enigma cipher machine



$$H_{enigma} = 65 \text{ or } 67$$

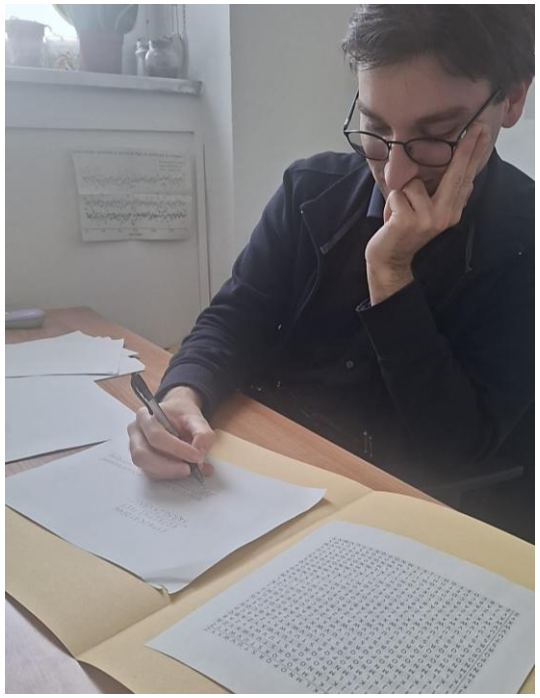
AES cipher

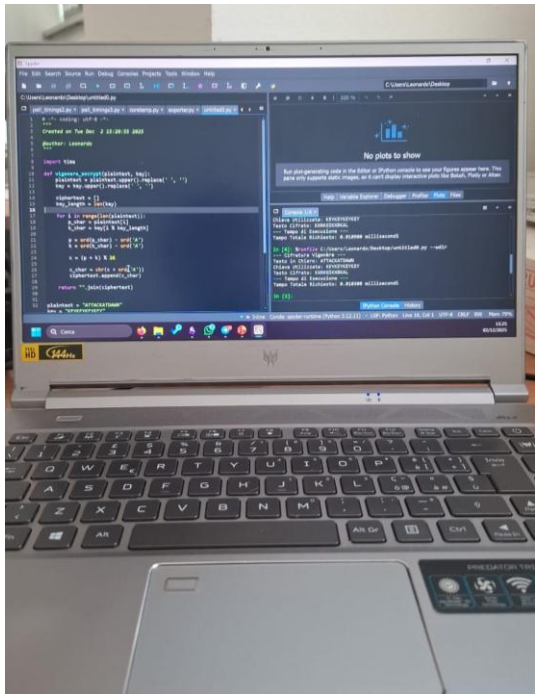


$\times$ 10 (or 12 or 14)

$H_{AES} = 128$ or 192 or 256

Good news





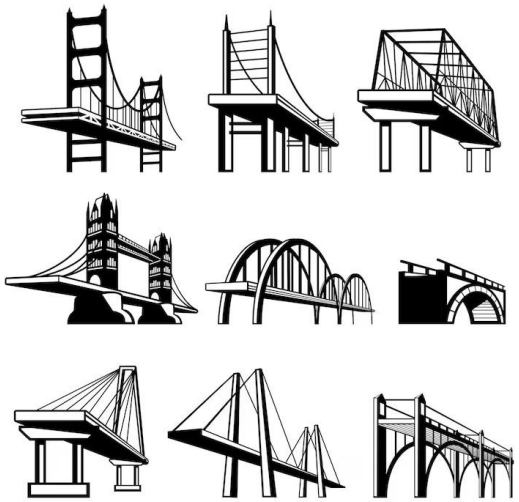
	me	**my laptop**
Vigenere	15 minutes	0.00001 seconds
AES-128	6 to 8 hours	0.00015 seconds

** benchmark on 128 characters*
*** photos by Francesco Turiano*

Bad news

1. Against entropy…
2. Machines themselves…
3. Contend in vain?

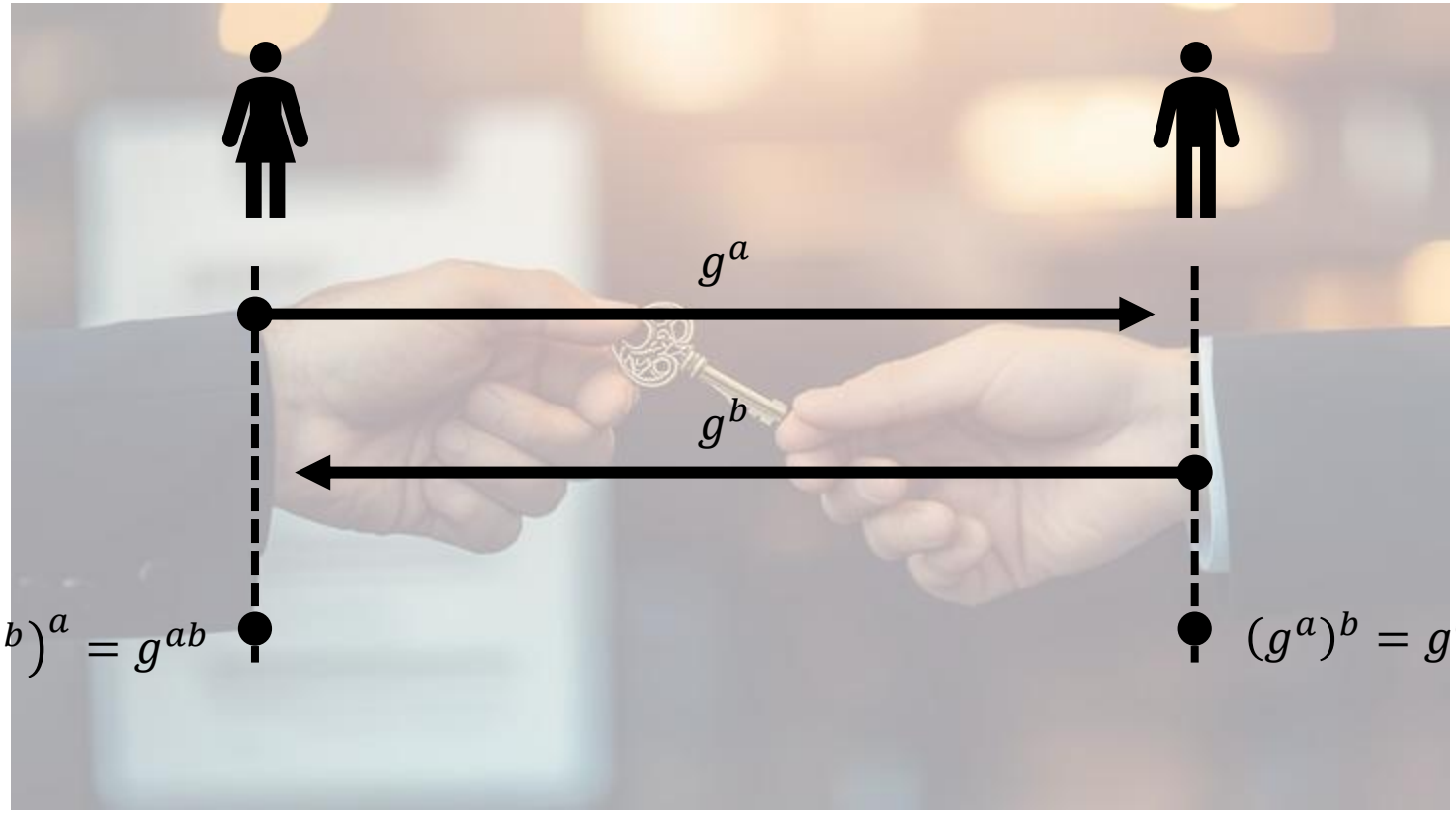
Security proofs



Security proofs

DH key exchange

DH key exchange



DH key exchange

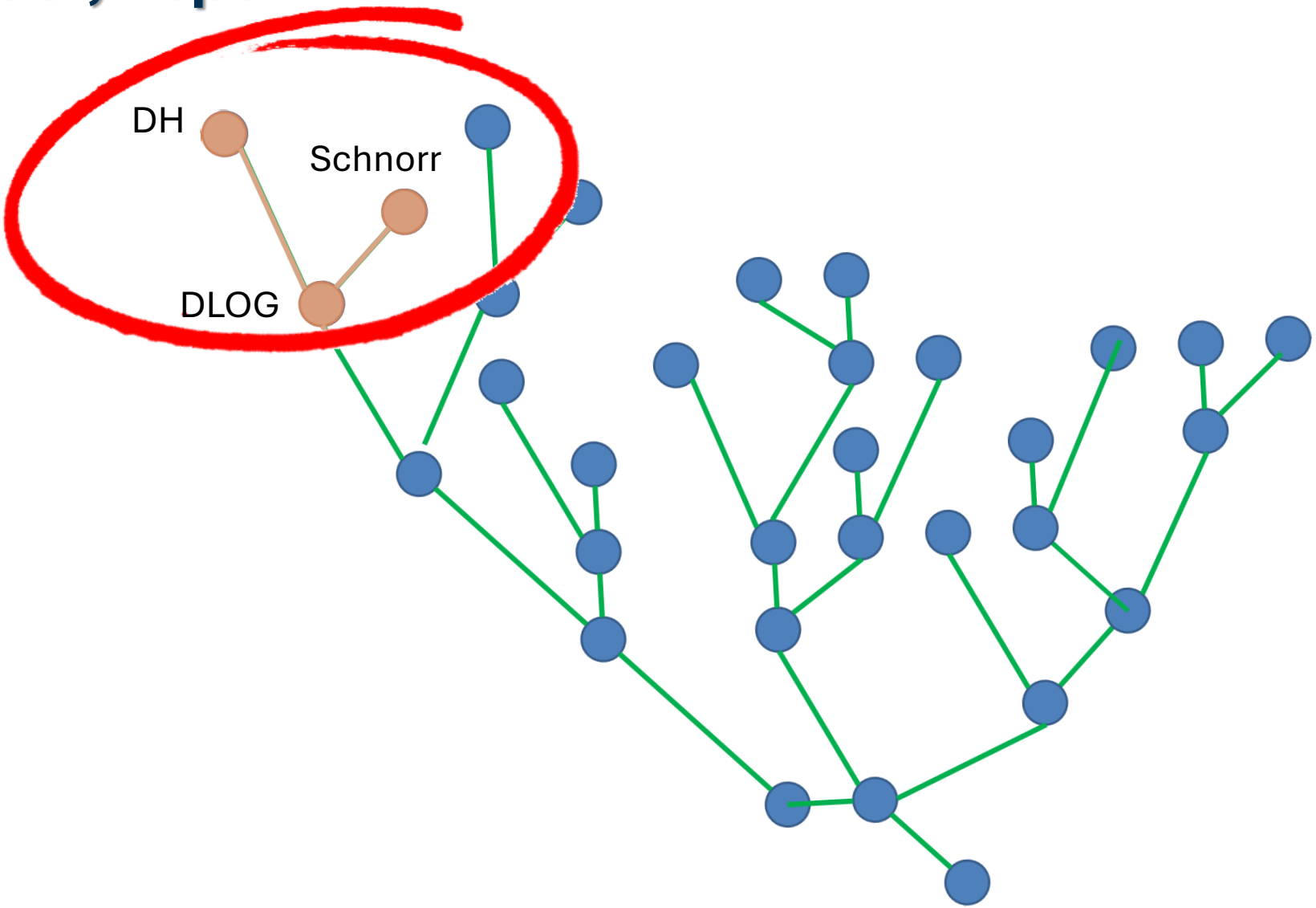
If DLOG is hard, DH is secure.

Discrete LOGarithm: given $g^x \in G$, find x.

DH security: cannot recover a or b.

If DH is not secure, DLOG is not hard.

At last, hope



“Get in, fair reader, into the depths of Cryptography.
Inspect the theory, view its foundations.
Is not the very core made of fine mathematics?”
- ***Gilgamesh***