CWI Centrum Wiskunde & Informatica

# CRYPTOGRAPHY

## Part I:
## Public-Key Cryptography


Serge Fehr

CWI Amsterdam
www.cwi.nl/~fehr

# Information…

- has become a **valuable resource**
- is the business model of many companies (G, f etc.)
- is nowadays almost always digitalized

  -> allows for easier use, but also for easier **misuse**
- **needs to be protected**

# Cryptography...

- is the mathematical study of info-protecting techniques
- provides tools for protecting information
- provides a **rigorous understanding** of
  - what security these tools achieve
  - what security these tools do **not** achieve
- is used in daily life by everybody - maybe unwittingly

# Secure Communication

ALICE


EVE

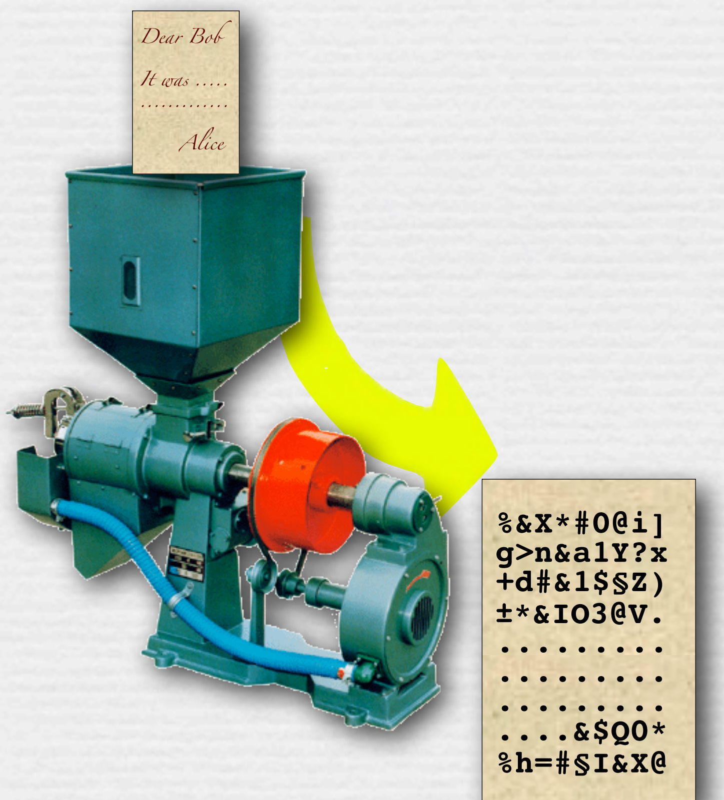
BOB

# Solution: Encryption

ALICE

EVE

BOB



# Solution: Encryption

# Solution: Encryption

ALICE

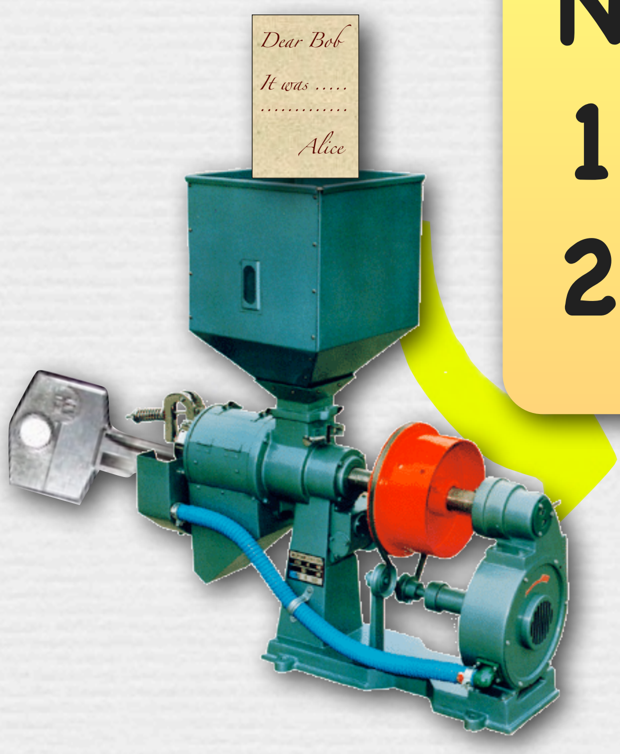
EVE

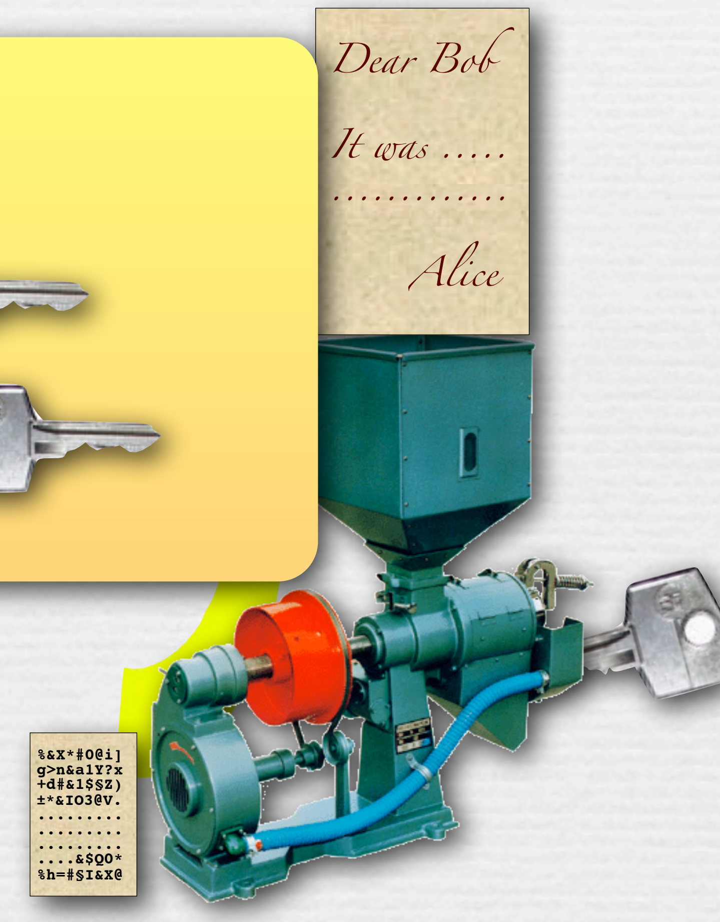

???

BOB

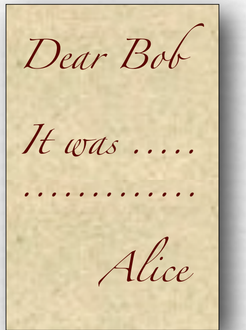
**Need:**

1. Alice & Bob know
2. Eve does not know



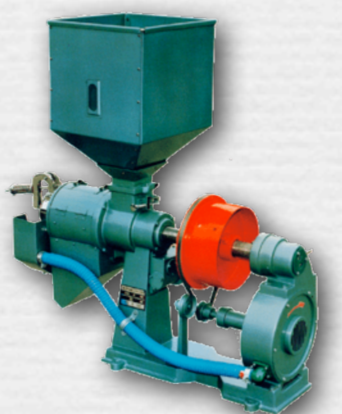



# “Dictionary”



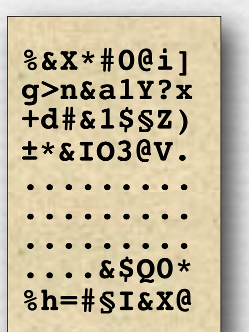

= electronic file / data: $m \in \mathcal{M}$

= en- & decryption key: $k \in \mathcal{K}$



= encryption function/procedure: $E_k : \mathcal{M} \rightarrow \mathcal{C}$

with corresponding decryption function: $E_k^{-1}$

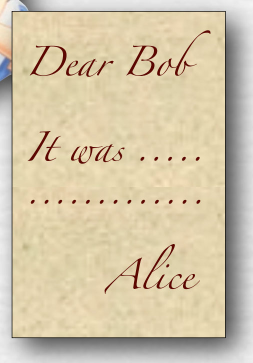



= encrypted file (= ciphertext): $c = E_k(m)$

and: $m = E_k^{-1}(c)$

# A (Even More) Mechanical View on Encryption

ALICE




EVE

BOB

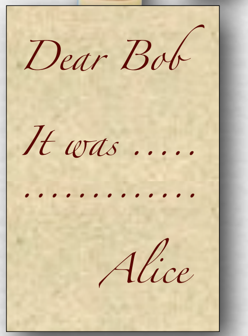
# A (Even More) Mechanical View on Encryption

ALICE

EVE

???

BOB




**Need:**

1. Alice & Bob know 
2. Eve does not know 

# Problem

ALICE


EVE

BOB

**But what if Alice & Bob have no common secret key**  **?**

# Problem


But what if Alice & Bob have no common secret key  ?

Sending the key from, e.g., Bob to Alice does not work, since then Eve learns it as well...

# A Mechanical Solution

ALICE


EVE

BOB

# A Mechanical Solution

ALICE

EVE

BOB

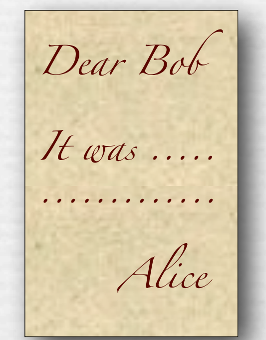
# A Mechanical Solution

ALICE

EVE

???

BOB




# Towards a Digital Solution




**Two** keys:
- a **public-key** to encrypt
- a **secret-key** to decrypt


# Towards a Digital Solution

# Towards a Digital Solution

# Towards a Digital Solution

# In Technical Terms

We need:

Encryption function $E_{pk}$, which depends on public-key $pk$, such that when given $pk$ (only):

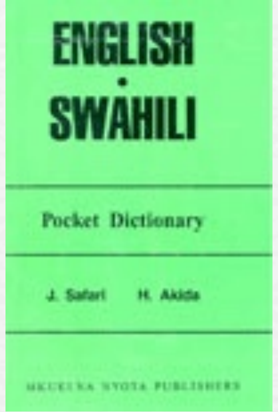
1. evaluating $E_{pk}(m)$ (on any $m$) is "easy", and
2. inverting $E_{pk}$, i.e., computing $m$ from $E_{pk}(m)$, is "hard".

With the help of a **trapdoor**, the secret-key $sk$, inverting $E_{pk}$ becomes "easy".

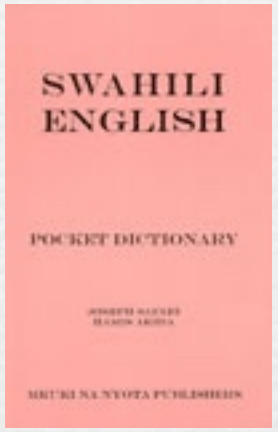
Is called a **trapdoor one-way function (TOWF)**.

# An "Toy Example" of a TOWF

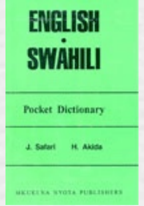
$pk$ = English-to-Swahili dictionary
(i.e. with the English entries sorted)




$sk$ = Swahili-to-English dictionary
(i.e. with the Swahili entries sorted)

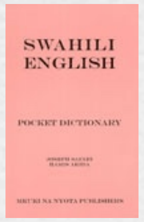



$E_{pk}(m)$ = translation of (English text) $m$ into Swahili

Given $pk$ = 

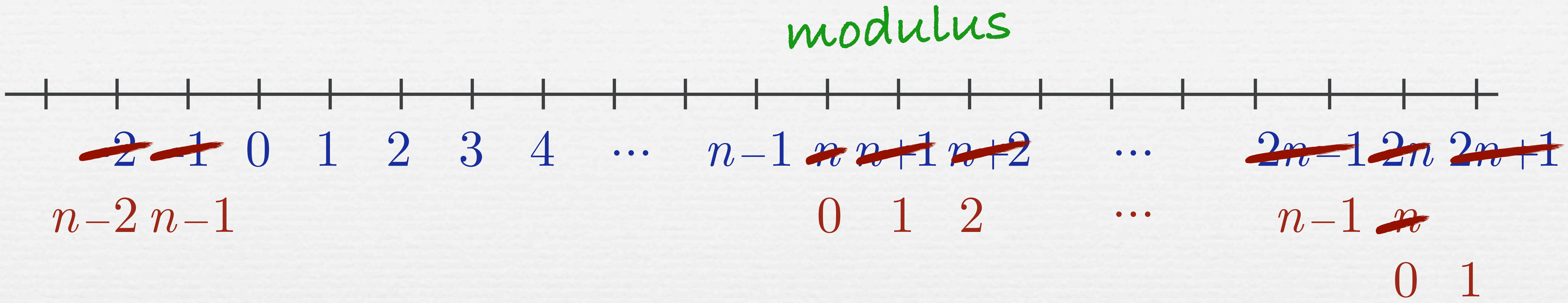
:

1. translating into Swahili (= computing $E_{pk}(m)$) is easy,
2. translating back into English (= inverting $E_{pk}$) is hard.

Yet with the help of 

, the latter becomes easy.

# Some Maths: Modular Arithmetic



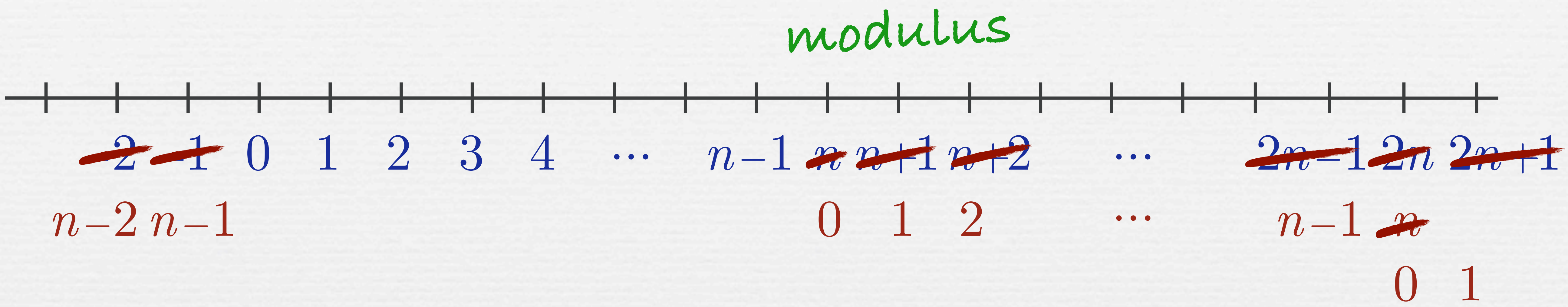

**Formally:** $a = b \pmod{n}$ if $a = b + k \cdot n$ for some $k$.

**Examples:** Set $n = 11$.

- $5 + 8 = 13 = 2 \pmod{11}$
- $5 \cdot 8 = 40 = 7 \pmod{11}$
- $2 \cdot 7 + 9 = 14 + 9 = 23 = 1 \pmod{11}$

  or $= 3 + 9 = 12 = 1 \pmod{11}$
- $4^3 = 4 \cdot 4 \cdot 4 = 16 \cdot 4 = 5 \cdot 4 = 20 = 9 \pmod{11}$

# Some Maths: Modular Arithmetic




**Formally**: $a = b \pmod{n}$ if $a = b + k \cdot n$ for some $k$.

**Examples**: Set $n = 11$.

- $5 + 8 = 13 = 2 \pmod{11}$

**Why is this interesting?**

- Numbers remain **bounded in size**
- Useful **structure**

- $4^3 = 4 \cdot 4 \cdot 4 = 16 \cdot 4 = 5 \cdot 4 = 20 = 9 \pmod{11}$

# Some Maths: Fermat's Little Theorem

Let $p$ be a **prime** number.

**Theorem**: For any number $a \neq 0$: $a^{p-1} = 1 \pmod{p}$ .

**Examples**: Let $p = 5$ and $a = 3$. Then

$$\begin{aligned} 3^4 &= 3 \cdot 3 \cdot 3 \cdot 3 = 9 \cdot 3 \cdot 3 = 4 \cdot 3 \cdot 3 \\ &= 12 \cdot 3 = 2 \cdot 3 = 6 = 1 \end{aligned} \qquad \pmod{5}$$

**Corollary**: If $x = y \pmod{p-1}$, then for any $a$:

$$a^x = a^y \pmod{p} .$$

**Proof**: $x = y \pmod{p-1} \Rightarrow x = y + k \cdot (p-1)$

$$\Rightarrow a^x = a^{y+k \cdot (p-1)} = a^y \cdot \left(a^{(p-1)}\right)^k = a^y \cdot 1^k = a^y \pmod{p}$$

# Some Maths: Euler's Theorem

Let $p$ be a **prime** number.

**Theorem**: For any number $a \neq 0$: $a^{p-1} = 1 \pmod{p}$ .

**Corollary**: If $x = y \pmod{p-1}$, then for any $a$:

$$a^x = a^y \pmod{p} .$$

Let $p$ and $q$ be two distinct **prime** numbers.

**Theorem**: For any number $a \neq 0$: $a^{(p-1)(q-1)} = 1 \pmod{pq}$.

**Corollary**: If $x = y \pmod{(p-1)(q-1)}$, then for any $a$:

$$a^x = a^y \pmod{pq} .$$

# A Real Example of a TWOF: RSA

Choose large (300-digits) prime numbers $p$ and $q$.
Compute $n = pq$ (easy to do).
Let $e$ be a (almost) arbitrary number, e.g. $e = 3$.

Set $pk = (n,e)$ and $sk = (p,q,e)$, and

$$E_{pk}(a) = a^e \pmod{n} \quad \text{(easy when given } pk\text{).}$$

Given $sk = (p,q,e)$, one can compute $d$ such that

$$de = 1 \pmod{(p-1)(q-1)} \quad \text{(ext. Euclid alg.)}$$

and then

$$E_{pk}(a)^d = (a^e)^d = a^{de} = a^1 = a \pmod{n}$$

# A Real Example of a TWOF: RSA

Choose large (300-digits) prime numbers $p$ and $q$.

Compute $n = pq$ (easy to do).

Let $e$ be a (almost) arbitrary num

Easy to compute when given $n$.

Set $pk = (n,e)$ and $sk = (p,q,e)$,

(easy when given $pk$).

Seemingly hard to compute knowing only $n$, but not $p$ & $q$.

te $d$ su

$(q-1))$ (ex

Easy to compute when given $p$ & $q$.

and then

$$E_{pk}(a)^d = (a^e)^d = a^{de} = a^1 = a \pmod{n}$$

# Finding TOWF's

Designing TOWF's / public-key encryption schemes is a **very challenging** task.

1976: Diffie & Hellman introduced the concept

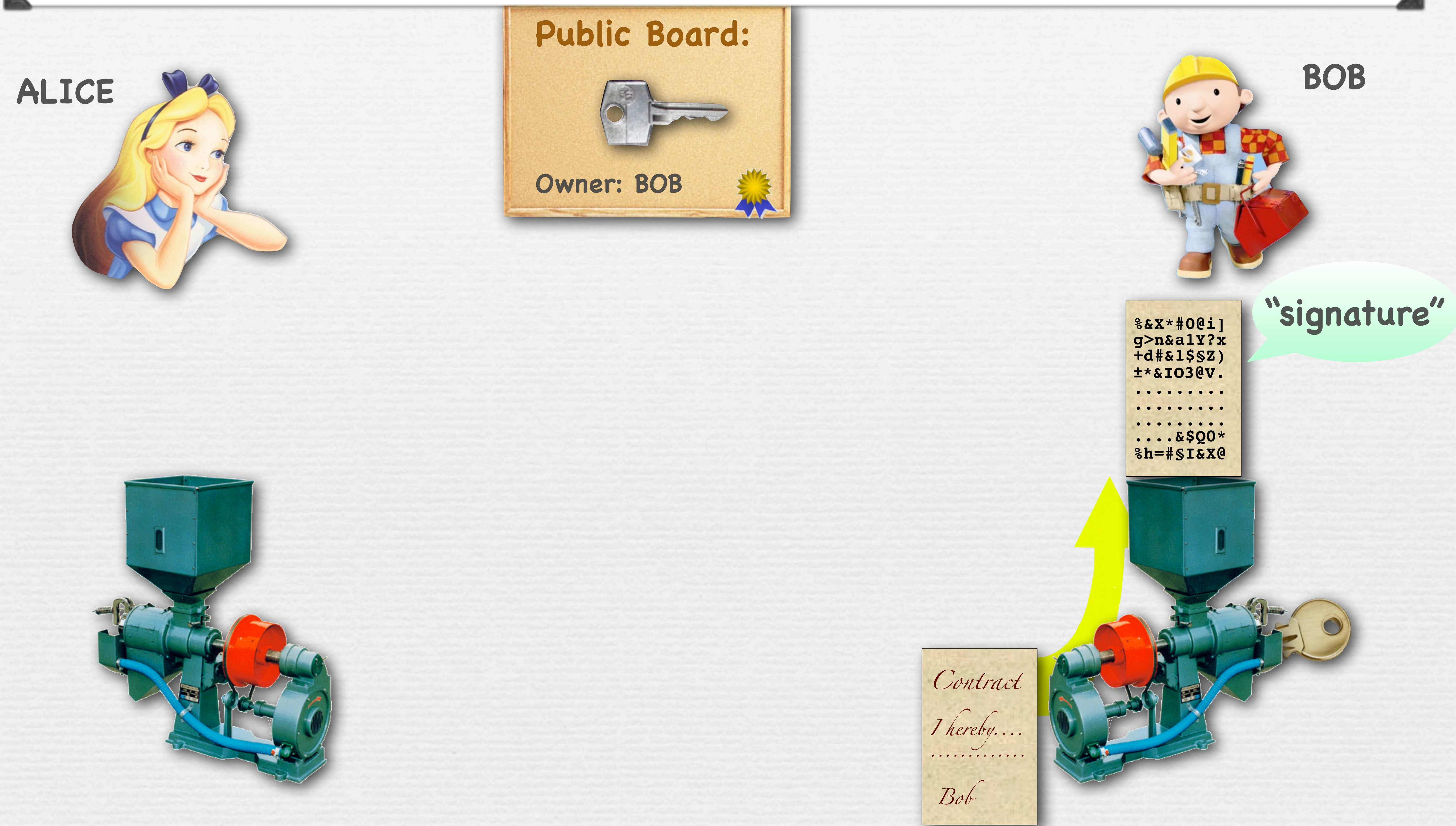
protects security of internet

1978: First example (RSA), by Rivest, Shamir & Adleman
(actually, by Clifford Cocks (GCHQ) in 1973)

1985: ElGamal encryption scheme, and elliptic-curve crypto

1996: Lattice-based schemes ("post-quantum crypto")

# Digital Signatures



# Digital Signatures

# Digital Signatures

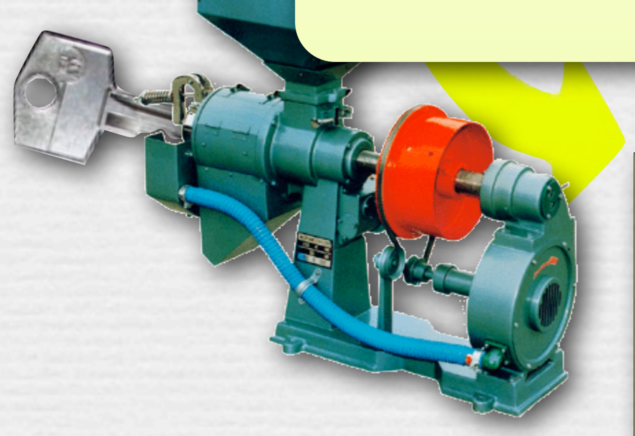
# Digital Signatures

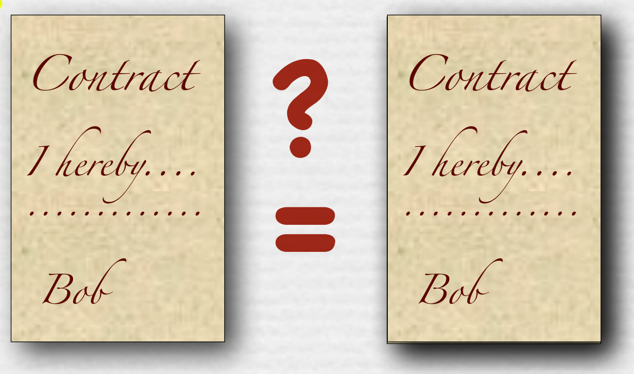
ALICE

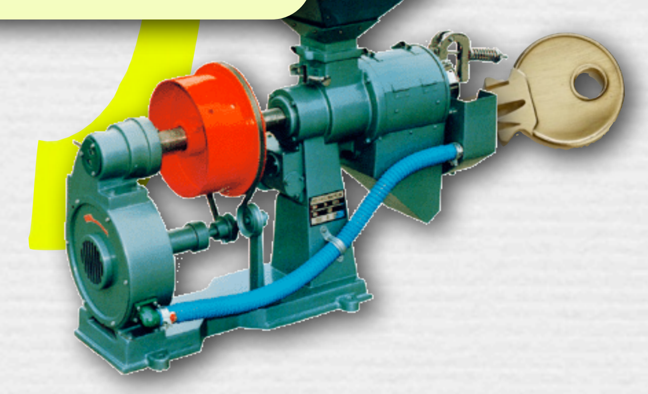

BOB

**Properties:**

Only **Bob** can **produce** a valid signature, but **everybody** can **verify** it.





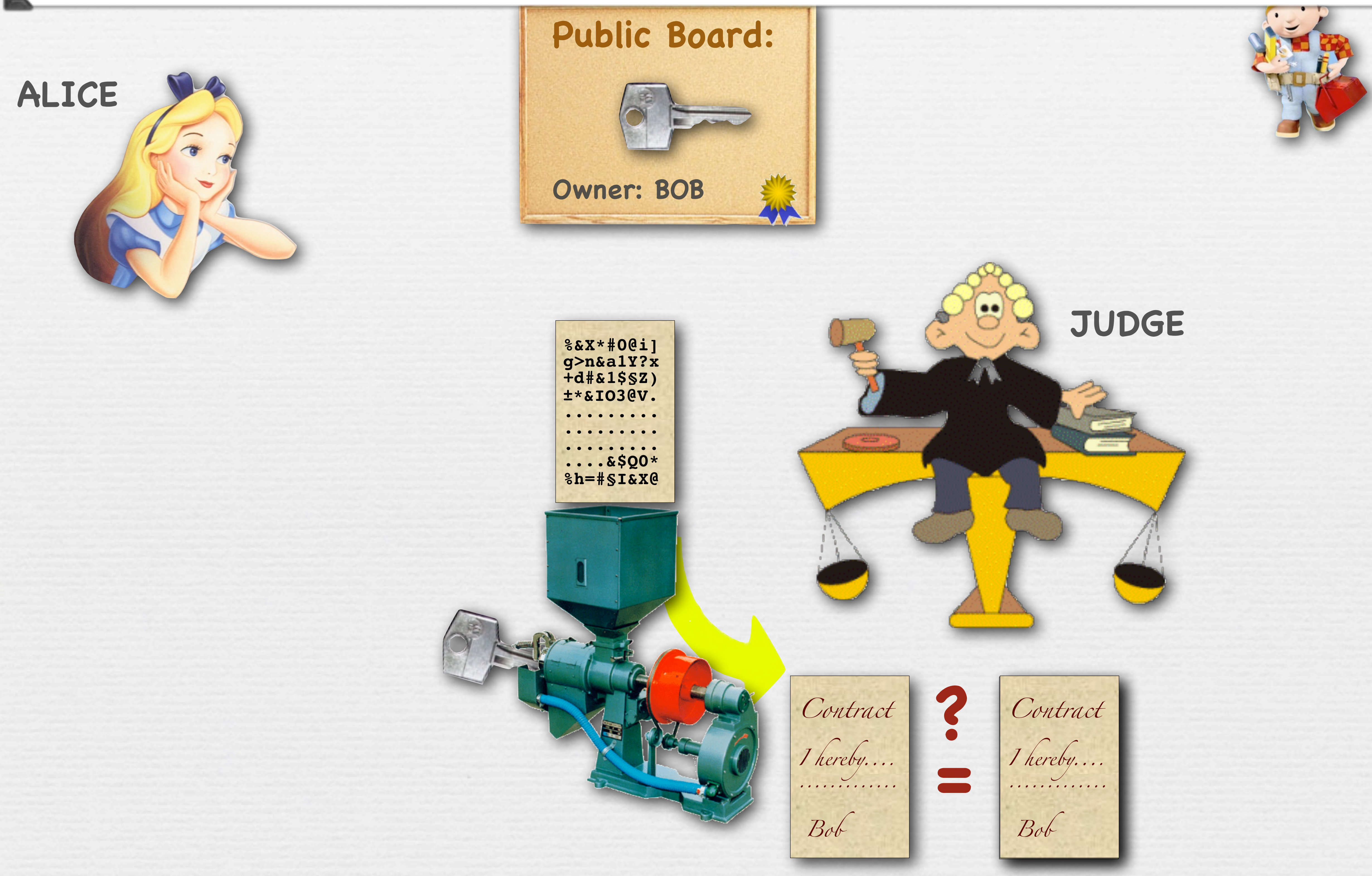
# Public Verifiability

ALICE



JUDGE

# Public Verifiability



# Internet Security

ALICE


# Internet Security

ALICE


Certification authorities (CA)

# Internet Security

ALICE


Entrust®
Securing Digital Identities & Information

digicert®

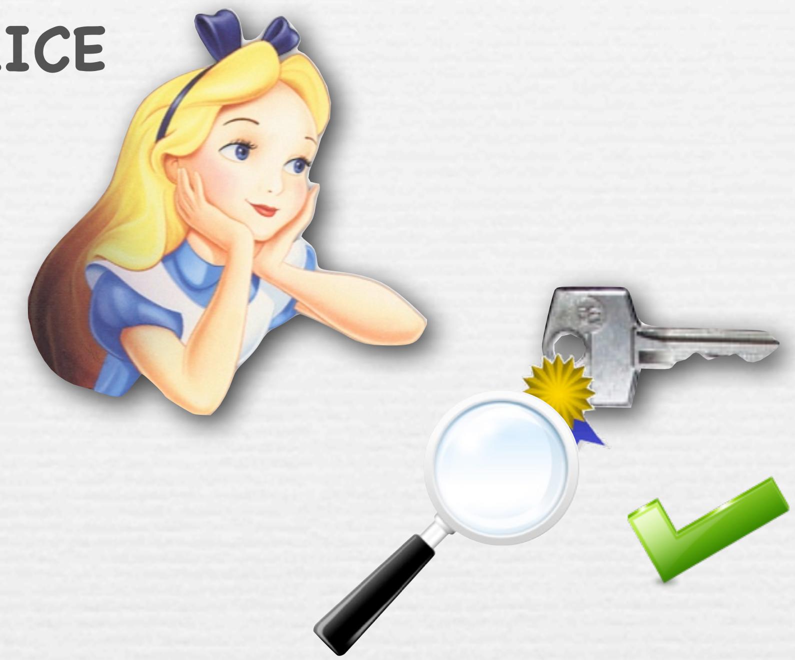
Symantec.

Deutsche Telekom

Certification authorities (CA)

# Internet Security

ALICE




Public keys of CA's are hard-coded into browser

Entrust
Securing Digital Identities & Information
digicert
Symantec.
Deutsche Telekom

Certification authorities (CA)

# Final Remarks

- (Public-key) cryptography offers powerful tools
- together with good understanding of their security
- **But:**
  - **applying** these tools correctly is often non-trivial
  - right **key-management** is crucial and tricky
  - the strongest lock is useless if not used properly