The Elliptic Curve in https

Marco Streng

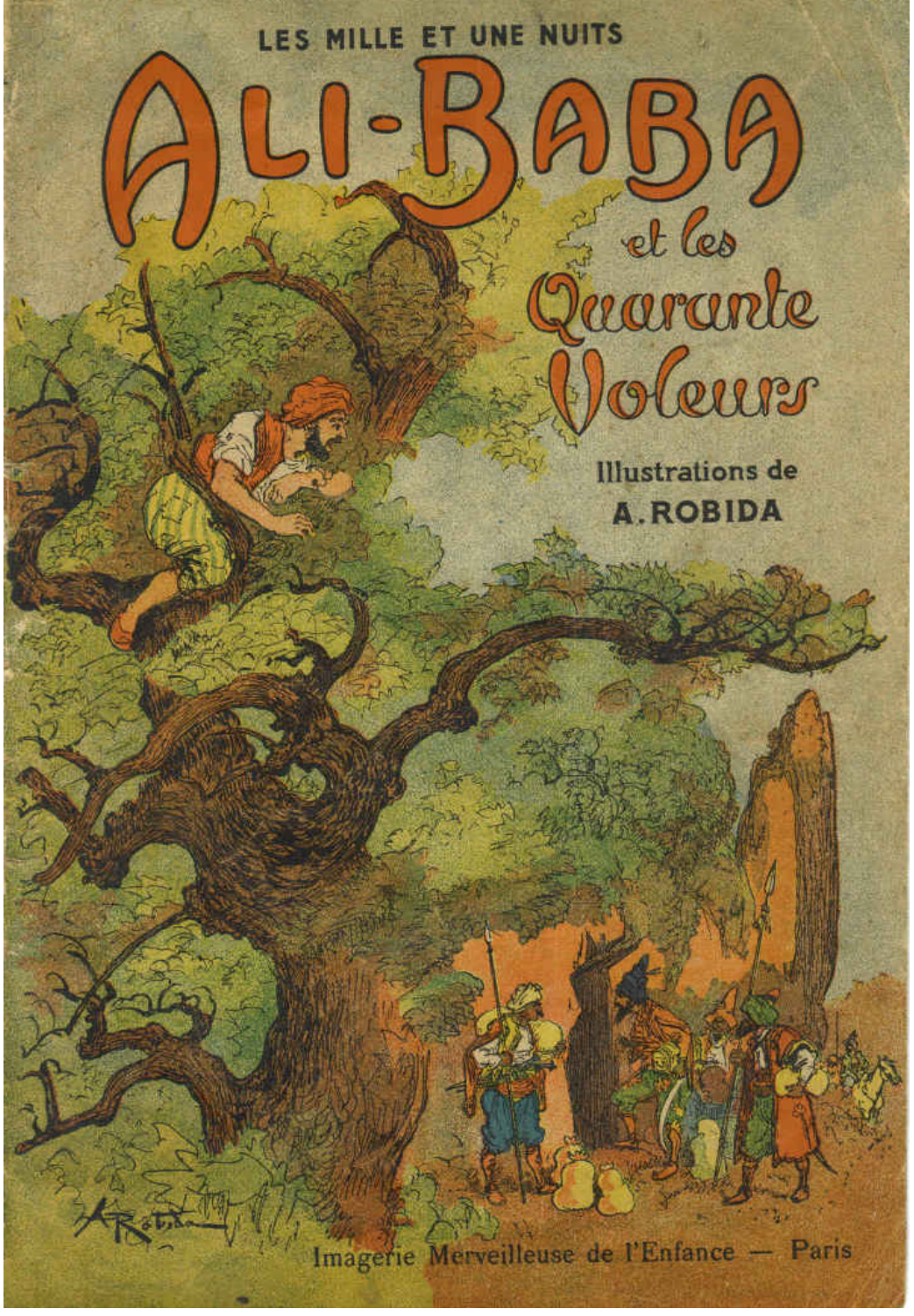
Universiteit Leiden

25 November 2014

LES MILLE ET UNE NUITS

Ali-Baba et les Quarante Voleurs

Illustrations de
A. ROBIDA



Imagerie Merveilleuse de l'Enfance — Paris


FREE
WiFi
FREE
WiFi
INSIDE
Free
WiFi
spot
FREE
WiFi
WiFi
FREE WiFi
Free
WiFi
spot
Wi·Fi
Here
Free
WiFi
spot
FREE
WiFi
FREE
WiFi
WiFi


FREE
WiFi
FREE
WiFi
INSIDE
Free
WiFi
spot
FREE
WiFi
WiFi
FREE WiFi
Free
WiFi
spot
Free
WiFi
spot
FREE
WiFi


FREE
WiFi
Free
WiFi
spot
FREE
WiFi
WiFi
FREE WiFi
Free
WiFi
spot
FREE
WiFi

The ‘s’ in ‘https://’

HyperText Transfer Protocol Secure

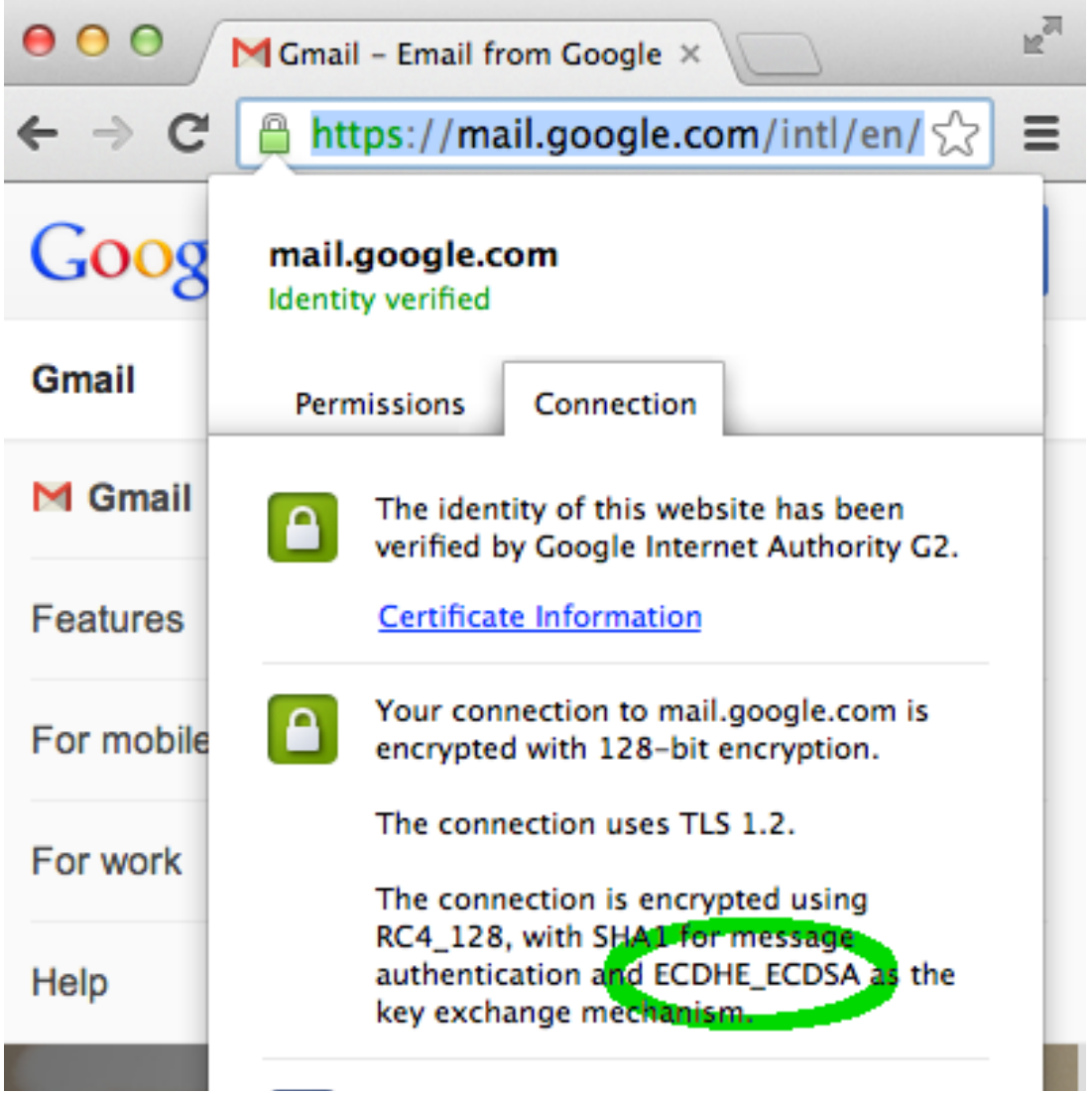
Uses algebra, number theory, and algebraic geometry to

- verify the identity of the web page (no fake cave)
- make sure communication is encrypted (no eavesdroppers)

Main players:

- RSA (see Algebra 1)
- Elliptic Curve Cryptography

Examples of use of ECC in the real world

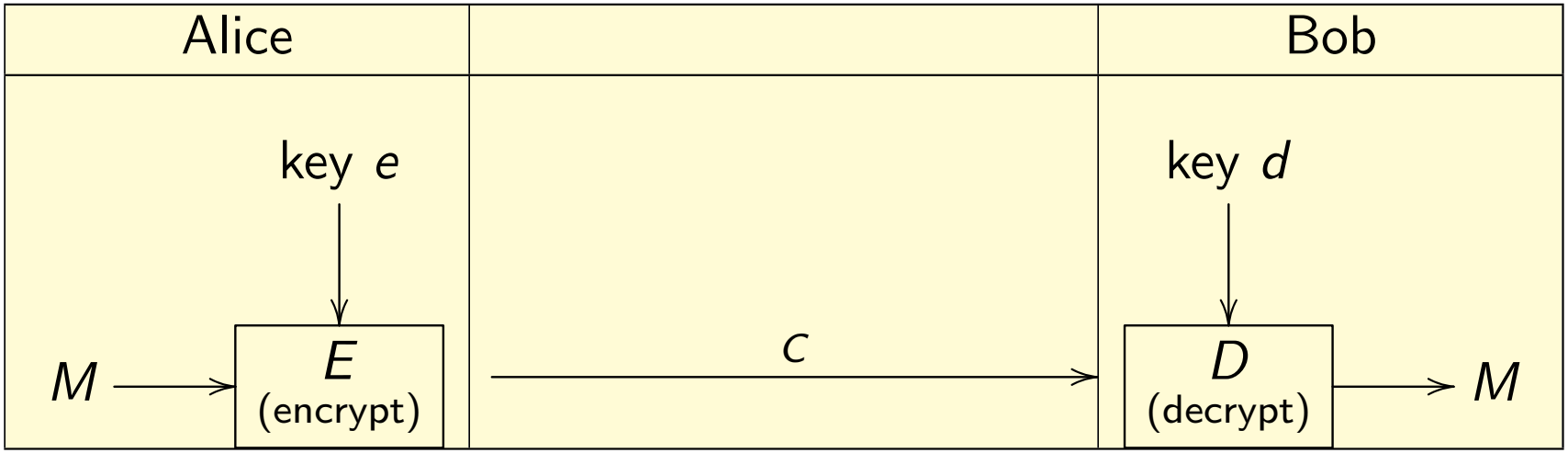


bitcoin

PS3

PlayStation 3

Encryption (protection against eavesdroppers)



Symmetric cryptography: one key $d = e = k$ is shared

Example: Caesar code

E shifts every letter forward by k in the alphabet

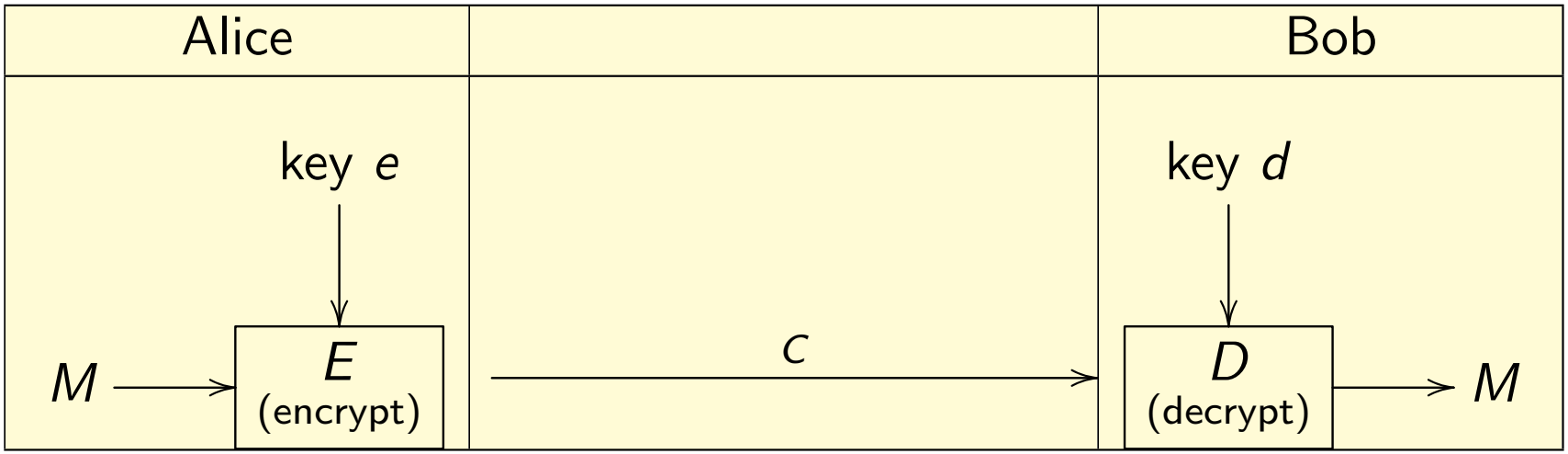
D shifts every letter backward by k in the alphabet

$k = 3$: DELFT $\rightarrow$ GHOIW $\rightarrow$ DELFT

More modern encryption (AES) is safe and fast, but...

need to share a key k first!

Asymmetric cryptography



Symmetric cryptography: one key $d = e = k$ is shared

Asymmetric cryptography: $d \neq e$; e is made public

Examples:

- everyone can encrypt messages that only Bob can read;
- Bob makes signatures that everyone can verify.

One way functions. Impossible?

The integers modulo 7

$$\mathbf{F}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$$

with the rules

$$\begin{aligned} \overline{x} + \overline{y} &= \overline{z}, && \text{where } z \text{ is remainder of } x + y \text{ on division by } 7 \\ \overline{x}\ \overline{y} &= \overline{z}, && \text{where } z \text{ is remainder of } x\ y \text{ on division by } 7 \end{aligned}$$

Examples:

$$\begin{aligned} \overline{3} + \overline{6} &= \overline{2} && \text{because } 3 + 6 = 9 = 1 \cdot 7 + 2 \\ \overline{5} \cdot \overline{4} &= \overline{6} && \text{because } 5 \cdot 4 = 20 = 2 \cdot 7 + 6 \\ \overline{2}^4 = \overline{2} \cdot \overline{2} \cdot \overline{2} \cdot \overline{2} &= \overline{2} \end{aligned}$$

Satisfies many rules of arithmetic such as $\overline{x}^{ab} = (\overline{x}^a)^b$.
(It is a ring.)

Exponentiation modulo 1000003

Examples of multiplication in $\mathbf{F}_{1000003}^* = \mathbf{F}_{1000003} \setminus \{\overline{0}\}$:

$$\begin{aligned}
\overline{1001}^2 &= \overline{1002001} = \overline{1998} \\
\overline{1001}^4 &= \overline{1998}^2 = \overline{991995} \\
\overline{1001}^8 &= \overline{991995}^2 = \cdots \\
\overline{1001}^{16} &= (\cdots)^2 = \cdots \\
\overline{1001}^{32} &= (\cdots)^2 = \cdots \\
\overline{1001}^{10000} &= ???? \\
10000 &= 2^{13} + 2^{10} + 2^9 + 2^8 + 2^4, \quad \text{so} \\
g^{10000} &= g^{(2^{13})} g^{(2^{10})} g^{(2^9)} g^{(2^8)} g^{(2^4)}.
\end{aligned}$$

Takes not 9999 multiplications, but only 17.

Exponentiation modulo $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$

Let $g \in \mathbf{F}_p$, $a \in \mathbf{Z}$ with 77 digits, say

$$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951,$$
$$g = \overline{40929056875212190070682550560009930198227808570709790430510819830666007717983},$$
$$a = 34045128435571965610752072282621814455526057737889900435563329387397872203496.$$

Computing $h = g^a$ takes not $3.4 \cdot 10^{76}$ multiplications in $\mathbf{F}_p$, but only ≤ 377. Phew!

So: easy to compute the map $a \mapsto g^a$.

Exponentiation modulo $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$

Let $g \in \mathbf{F}_p$, $a \in \mathbf{Z}$ with 77 digits,

$$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951,$$
$$g = \overline{40929056875212190070682550560009930198227808570709790430510819830666007717983},$$
$$a = 34045128435571965610752072282621814455526057737889900435563329387397872203496.$$

Computing $h = g^a$ takes not $3.4 \cdot 10^{76}$ multiplications in $\mathbf{F}_p$, but only ≤ 377. Phew!

So: easy to compute the map $a \mapsto g^a$.

Inverse?
Given g and $h = g^a$, find a. (Discrete log problem (DLP) in $\mathbf{F}_p^*$)

Naive algorithm: try $g^1 = h?$, $g^2 = h?$, $g^3 = h?$, ...
Need $\approx 3.4 \cdot 10^{76}$ tries to find a.
Takes impossibly long!

We have our one way map: $a \mapsto g^a$.

Exponentiation modulo $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$

Given g and $h = g^a$, find a. (Discrete log problem (DLP) in $\mathbf{F}_p^*$)

Naive algorithm: try $g^1 = h?$, $g^2 = h?$, $g^3 = h?$, ...
Need $\approx 3.4 \cdot 10^{76}$ tries to find a.
Takes impossibly long!

We have our one way map: $a \mapsto g^a$.

There exist encryption and digital signatures based on the DLP.

Instead, I will explain a simpler cryptographic protocol.

Diffie-Hellman key exchange (1976)

Goal: agree on a key for symmetric encryption

Public parameters: p a prime number, $g \in \mathbf{F}_p^*$.

Alice	(communication channel)	Bob
random $a \in \mathbf{Z}$ compute g^a	g^a → ← g^b	random $b \in \mathbf{Z}$ compute g^b
compute $g^{(ab)} = (g^b)^a$ and use as key		compute $g^{(ab)} = (g^a)^b$ and use as key

- Given only p, g, g^a, g^b, it is believed to be hard to find $g^{(ab)}$.
- Finding a is the discrete logarithm problem in $\mathbf{F}_p^*$, and breaks the scheme.

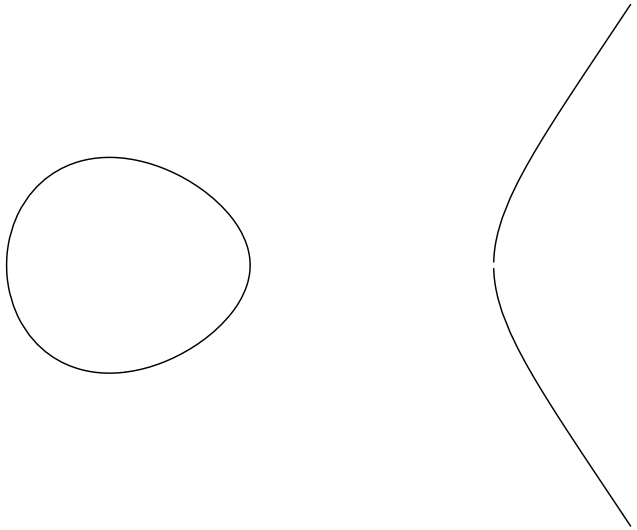
Elliptic curves

Next: what are elliptic curves, and why are they better?

Elliptic curves

- Consider the curve in the (x, y)-plane $\mathbf{R}^2$ given by the equation

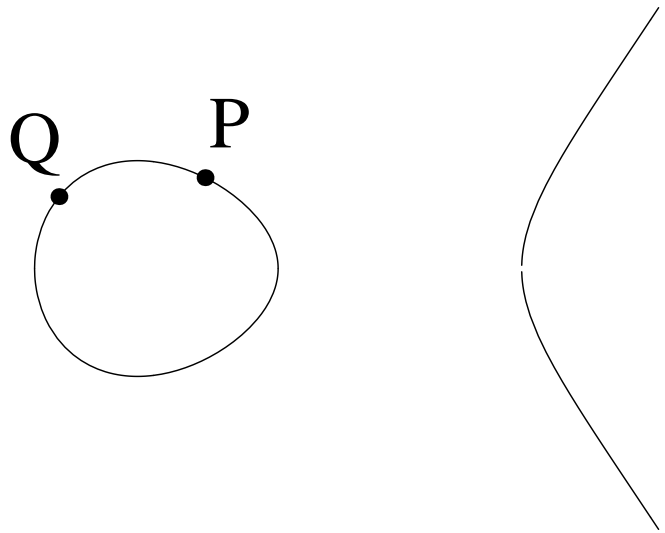
$$y^2 = x^3 - 3x.$$



Elliptic curves

- Consider the curve in the (x, y)-plane $\mathbf{R}^2$ given by the equation

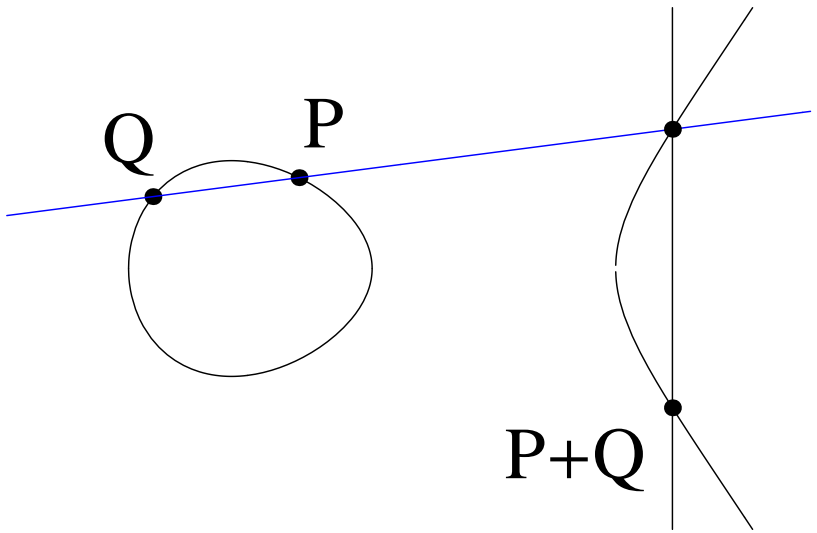
$$y^2 = x^3 - 3x.$$



Elliptic curves

- Consider the curve in the (x, y)-plane $\mathbf{R}^2$ given by the equation

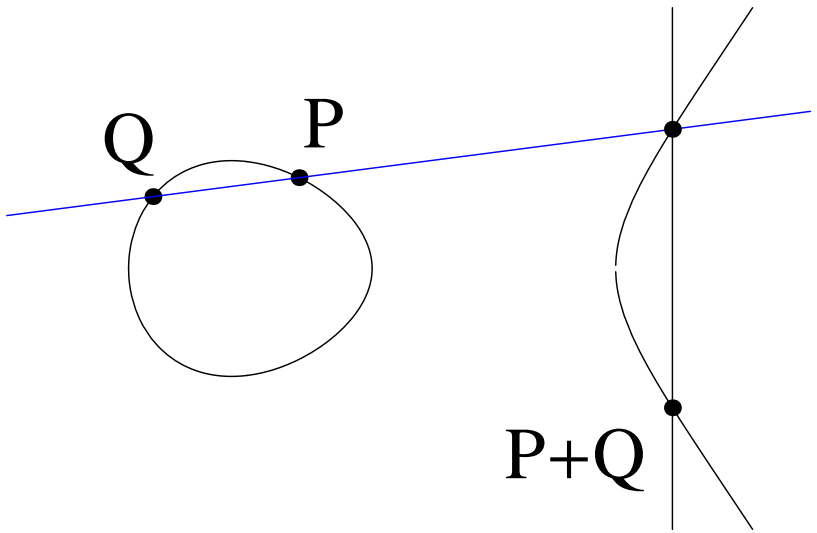
$$y^2 = x^3 - 3x.$$



Elliptic curves

- Consider the curve in the (x, y)-plane $\mathbf{R}^2$ given by the equation

$$y^2 = x^3 - 3x.$$



- We get an addition law "+" on the set $E(\mathbf{R})$ of points, including one extra point 0 "at infinity".
- "+" satisfies standard rules of arithmetic such as $(P + Q) + R = P + (Q + R)$ ($E(\mathbf{R})$ is a "group").
- $nP = P + P + \cdots + P$

Formulas (up to typos)

Given $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(\mathbf{R})$.
If $x_1 = x_2$ and $y_1 = -y_2$, then $P + Q = 0$.
Otherwise,

$$P + Q = (x_3, y_3),$$

where:
If $x_1 \neq x_2$, then

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \quad y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1};$$

If $x_1 = x_2$, then

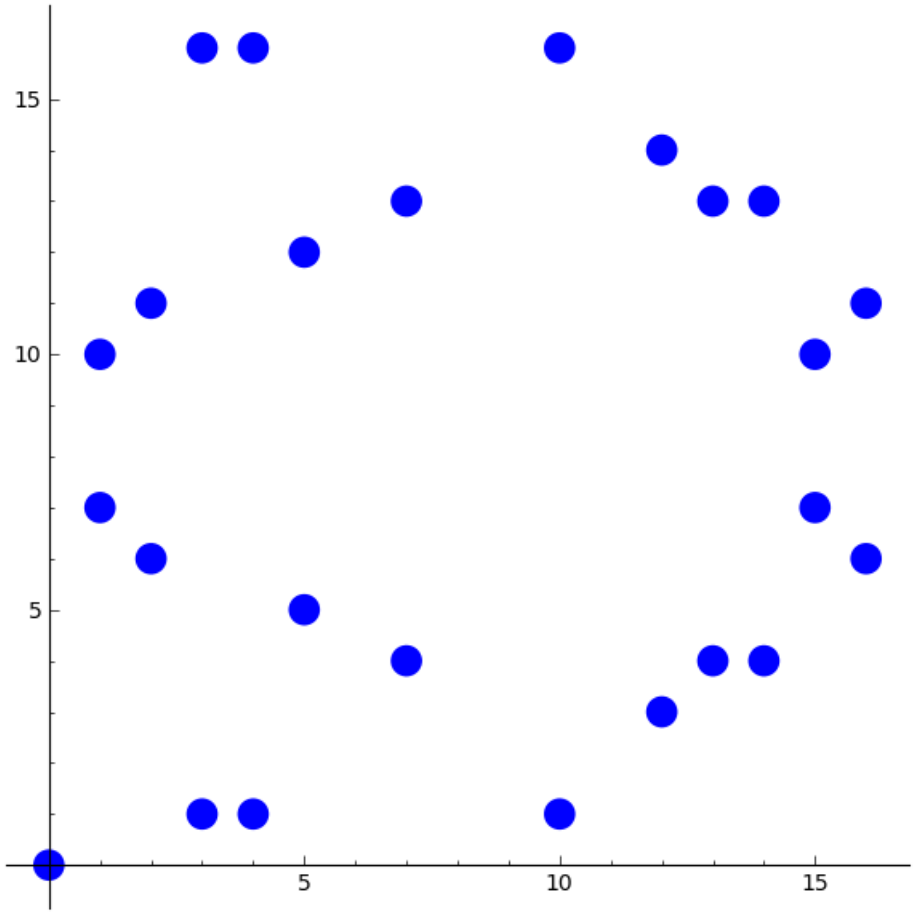
$$x_3 = \frac{(x^2 + 3)^2}{4x(x^2 - 3)}, \quad y_3 = \frac{3x_3(x^2 - 1) + x^3 + 3x}{-2y_1}.$$

So defining E and $+$ only uses arithmetic.
In particular, we can define elliptic curves over $\mathbf{F}_p$ and add points on them!

Elliptic curves over $\mathbf{F}_p$

Defining E and $+$ only uses arithmetic.
In particular, we can define elliptic curves over $\mathbf{F}_p$ and add points on them!

Example:
$y^2 = x^3 - \overline{3}x$ over $\mathbf{F}_{17}$.
$G = (\overline{3}, \overline{1}) \in E(\mathbf{F}_{17})$
(as $\overline{1}^2 = \overline{3}^3 - \overline{3} \cdot \overline{3}$)



The elliptic curve discrete logarithm problem

Example: $y^2 = x^3 - \overline{3}x$ over $\mathbf{F}_{17}$.

$G = (\overline{3}, \overline{1}) \in E(\mathbf{F}_{17}) \qquad (\text{as } \overline{3}^2 - \overline{3} \cdot \overline{3} = \overline{1}^2)$

$$\begin{aligned} 2G &= (\overline{2}, \overline{11}) \\ 4G &= 2(2G) = (\overline{4}, \overline{16}) \\ 8G &= 2(4G) = (\overline{1}, \overline{10}) \\ 16G &= 2(8G) = (\overline{15}, \overline{7}) \end{aligned}$$

So $18G = 16G + 2G = (\overline{1}, \overline{7})$ takes not 17 but only 6 additions.

Now suppose $p \approx 2^{256}$. Computing aG with $a \approx 2^{256} \approx 10^{77}$ takes not 10^{77} additions but less than 500.

The elliptic curve discrete log problem asks:
given p, E, $G \in E(\mathbf{F}_p)$, $H = aG$, compute a.

Diffie-Hellman key exchange (1976)

Goal: agree on a key for symmetric encryption

Public parameters: p a prime number, $g \in \mathbf{F}_p^*$.

Alice	(communication channel)	Bob
random $a \in \mathbf{Z}$ compute g^a	g^a → ← g^b	random $b \in \mathbf{Z}$ compute g^b
compute $g^{(ab)} = (g^b)^a$ and use as key		compute $g^{(ab)} = (g^a)^b$ and use as key

- Given only p, g, g^a, g^b, it is believed to be hard to find $g^{(ab)}$.
- Finding a is the discrete logarithm problem in $\mathbf{F}_p^*$, and breaks the scheme.

Elliptic Curve cryptography, Koblitz and Miller (1985)

Replace $\mathbf{F}_p^*$ by $E(\mathbf{F}_p)$ in any discrete log cryptosystem, e.g.:

Public parameters: p a prime number, E elliptic curve, $G \in E(\mathbf{F}_p)$.

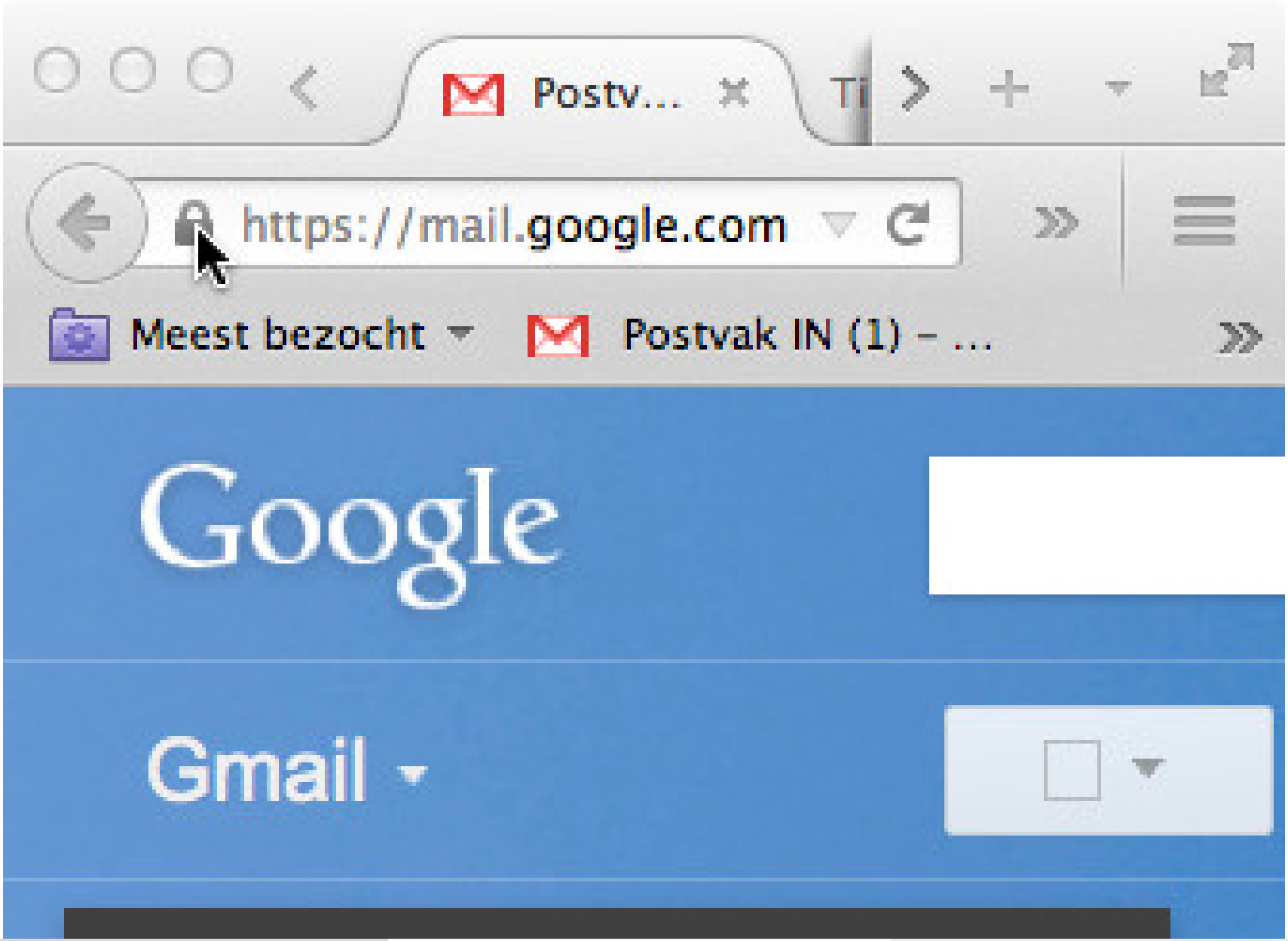
Alice	(communication channel)	Bob
random $a \in \mathbf{Z}$ compute aG	aG → ← bG	random $b \in \mathbf{Z}$ compute bG
compute $(ab)G = a(bG)$ and use as key		compute $(ab)G = b(aG)$ and use as key

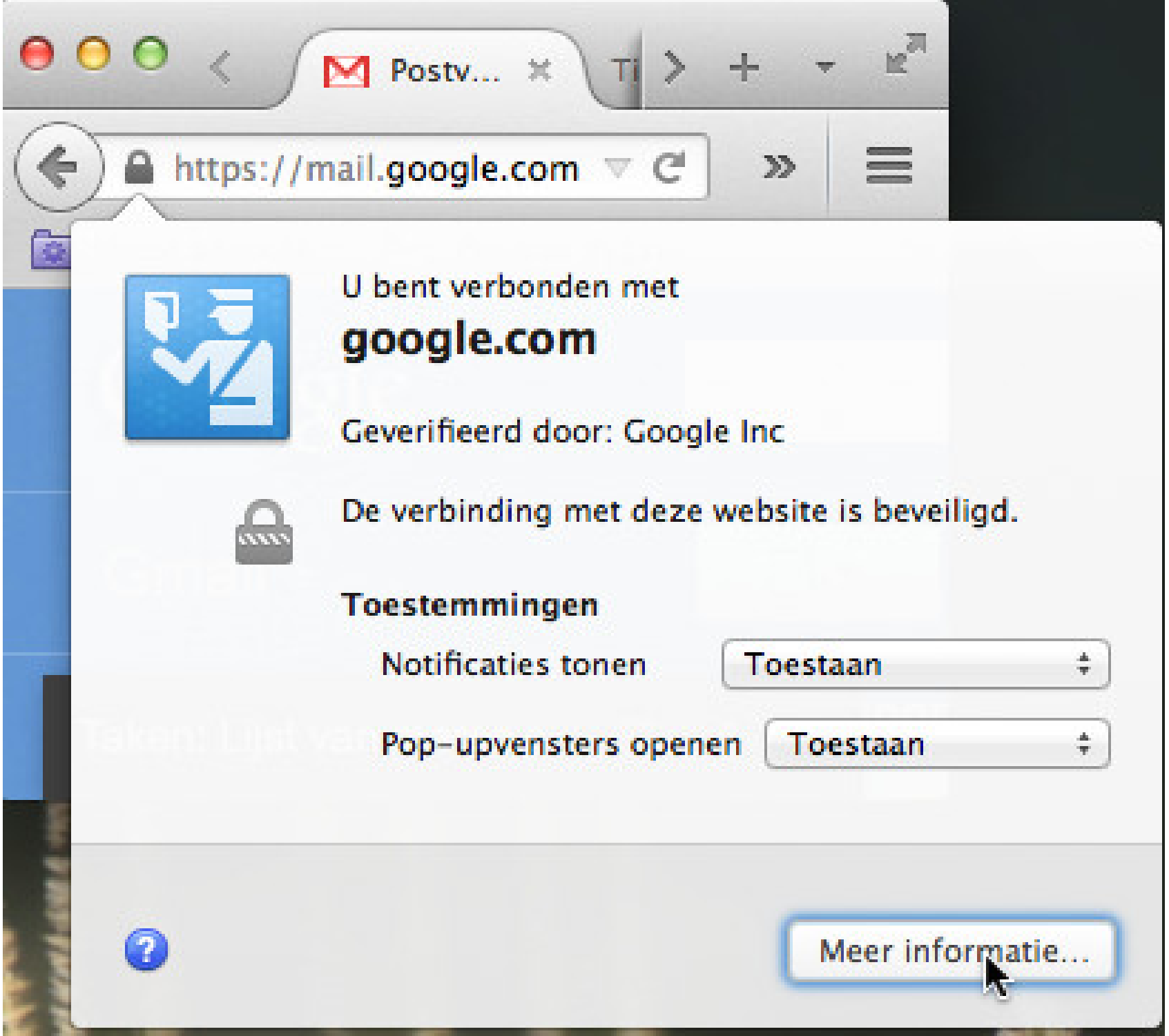
- Given only E, G, aG, bG, it is believed to be hard to find $(ab)G$.
- Finding a is the discrete logarithm problem in $E(\mathbf{F}_p)$, and breaks the scheme.

Fast attacks

- So far, only mentioned naive attack:
  try $a = 1$, $a = 2$, $a = 3$, ...
- There exist much faster methods for solving the discrete log problem in $\mathbf{F}_p^*$ based on algebraic geometry and algebraic number theory.
- To make these attacks infeasible, for $\mathbf{F}_p^*$-cryptography use not $p \approx 2^{256}$ (77 digits), but use $p \approx 2^{3072}$ (924 digits).
- For EC discrete logs, no fast attacks are known (in spite of much effort!), and working with 77 digits is safe.
- This makes ECC much more efficient at the same security level!

Example: Gmail (screenshots of Firefox)




Postv...
https://mail.google.com
U bent verbonden met
google.com
Geverifieerd door: Google Inc
De verbinding met deze website is beveiligd.
Toestemmingen
Notificaties tonen
Toestaan
Pop-upvensters openen
Toestaan
Meer informatie...

Pagina-info – https://mail.google.com/mail/u/0/?shva=1#inbox

Algemeen | Media | Feeds | Toestemmingen | Beveiliging

Website-identiteit

Website:	**mail.google.com**
Eigenaar:	**Deze website verstrekt geen eigendomsinformatie.**
Geverifieerd door:	**Google Inc**

Certificaat bekij

Privacy & geschiedenis

Heb ik deze website eerder dan vandaag bezocht?	**Ja, 13,157 maal**	
Slaat deze website informatie (cookies) op op mijn computer?	**Ja**	Cookies bekij
Heb ik wachtwoorden opgeslagen voor deze website?	**Nee**	Opgeslagen wachtwoorden bekij

Technische details

Beveiligde verbinding: hoge graad van versleuteling (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128-bits sleu

De pagina die u bekijkt was beveiligd voordat deze over het internet werd verzonden.

Versleuteling maakt het erg moeilijk voor onbevoegde personen om informatie te bekijken die tussen computers wordt uitgewisseld. Het is daarom erg onwaarschijnlijk dat iemand deze pagina heeft gelezen terwijl hij over het netwerk werd verzonden.

Certificaatweergave:"mail.google.com"

Algemeen | Details

Certificaathiërarchie

- Builtin Object Token:Equifax Secure CA
  - GeoTrust Global CA
    - Google Internet Authority G2
      - mail.google.com

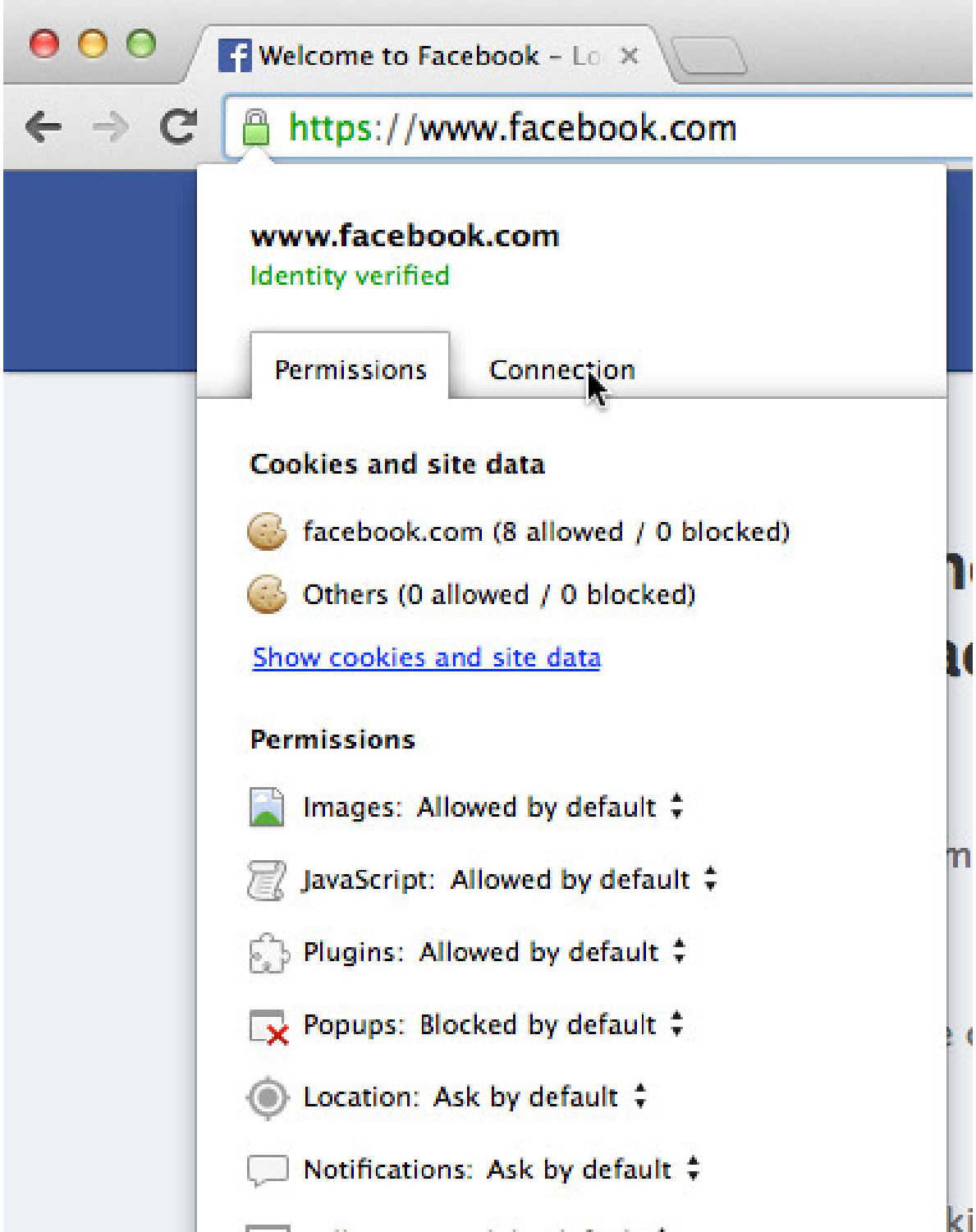
Certificaatvelden

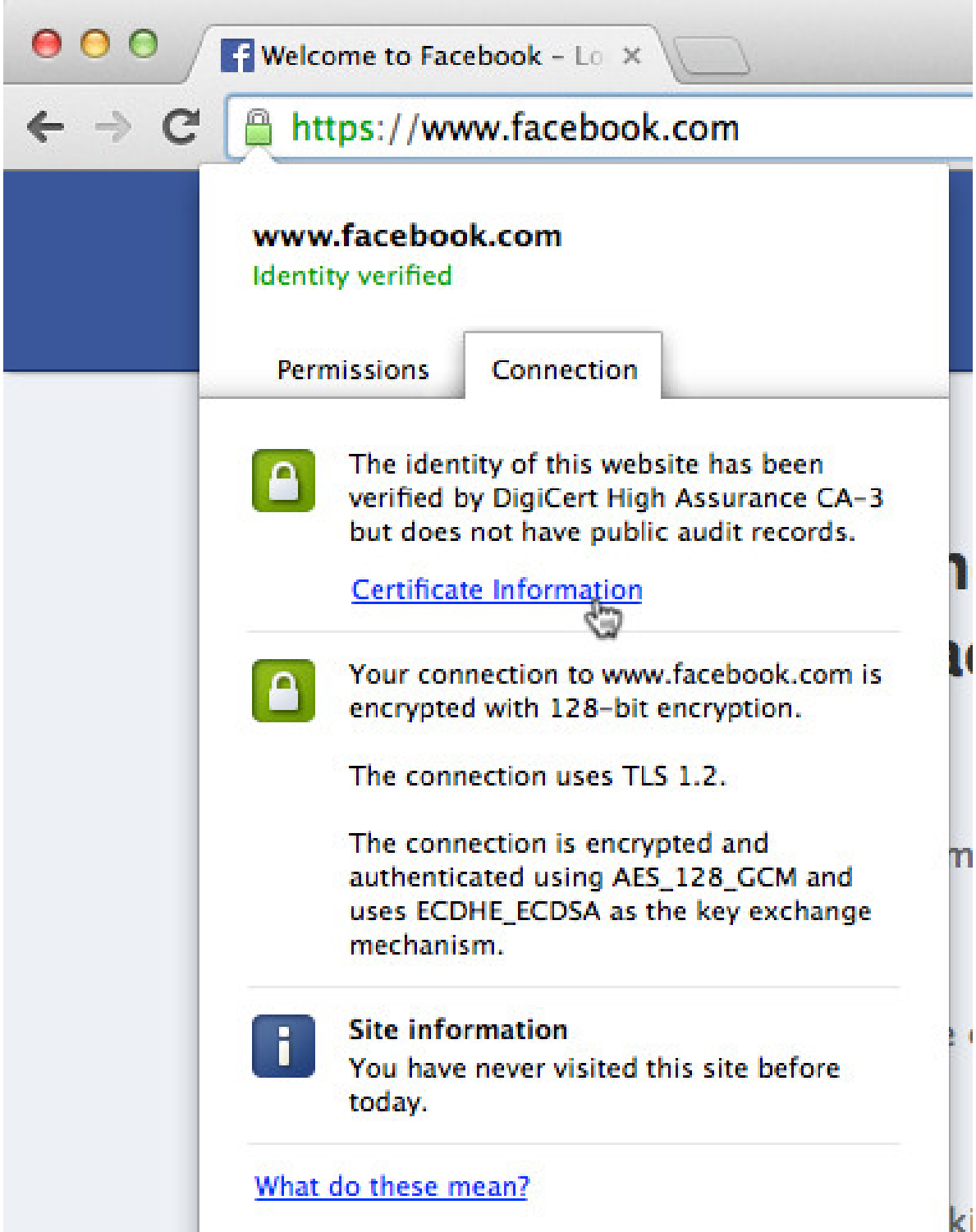
- Niet voor
- Niet na
- Certificaathouder
- Info over publieke sleutel van certificaathouder
  - Algoritme van publieke sleutel van certificaathouder
    - Algoritme-identificator
    - Algoritmeparameters
  - Publieke sleutel van certificaathouder
- Extensies

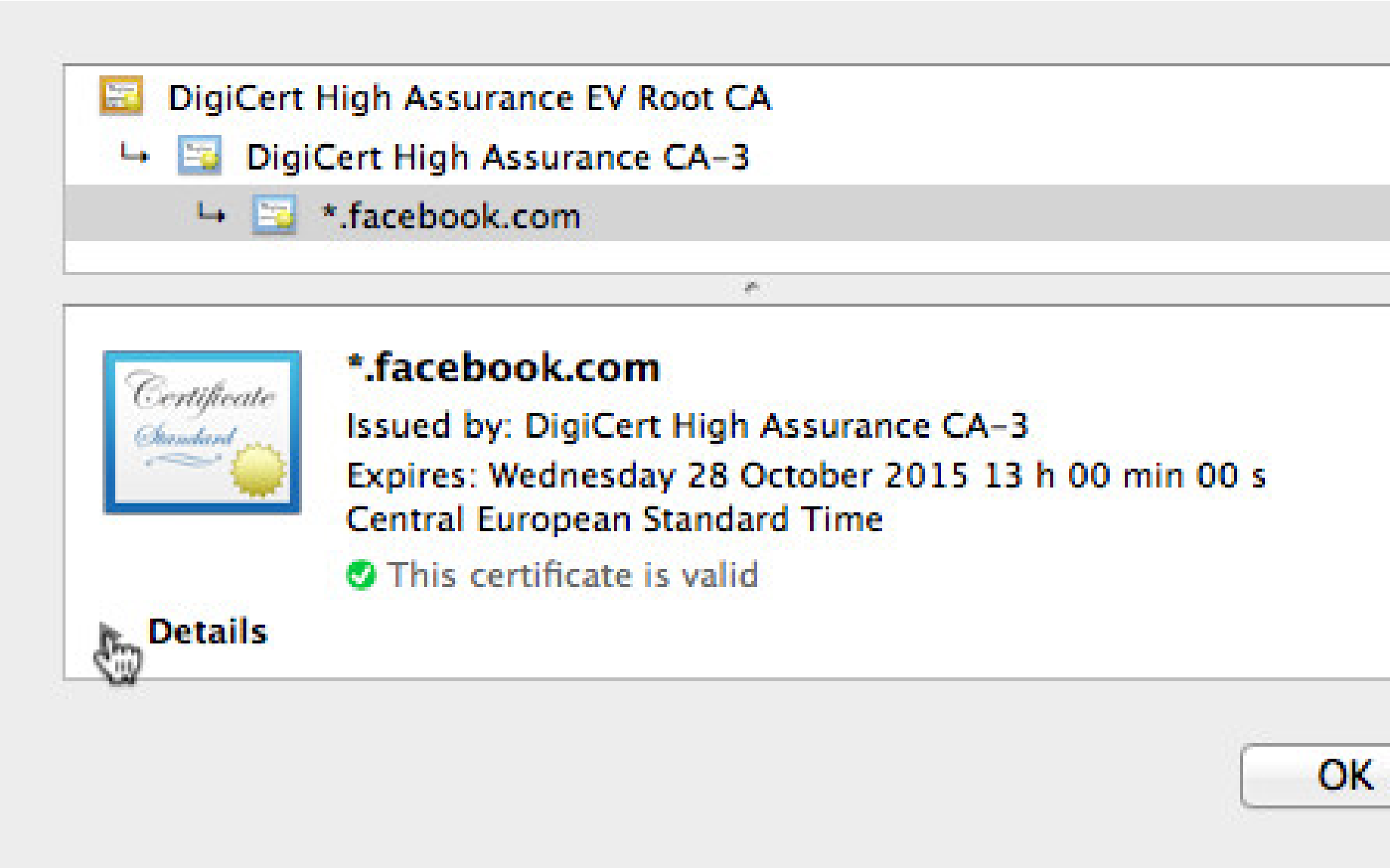
Veldwaarde

```
ANSI X9.62 elliptische kromme prime256v1 (aka secp256r1, NIST P-256)
```

Example: Facebook (screenshots of Chrome)


Welcome to Facebook - Lo
https://www.facebook.com
www.facebook.com
Identity verified
Permissions
Connection
Cookies and site data
facebook.com (8 allowed / 0 blocked)
Others (0 allowed / 0 blocked)
Show cookies and site data
Permissions
Images: Allowed by default
JavaScript: Allowed by default
Plugins: Allowed by default
Popups: Blocked by default
Location: Ask by default
Notifications: Ask by default


Welcome to Facebook - Lo
https://www.facebook.com
www.facebook.com
Identity verified
Permissions
Connection
The identity of this website has been verified by DigiCert High Assurance CA-3 but does not have public audit records.
Certificate Information
Your connection to www.facebook.com is encrypted with 128-bit encryption.
The connection uses TLS 1.2.
The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_ECDSA as the key exchange mechanism.
Site information
You have never visited this site before today.
What do these mean?


DigiCert High Assurance EV Root CA
DigiCert High Assurance CA-3
*.facebook.com
Certificate
Standard
*.facebook.com
Issued by: DigiCert High Assurance CA-3
Expires: Wednesday 28 October 2015 13 h 00 min 00 s
Central European Standard Time
This certificate is valid
Details
OK

DigiCert High Assurance EV Root CA

↳ DigiCert High Assurance CA-3

↳ *.facebook.com

Not Valid Before	Thursday 28 August 2014 02 h 00 min 00 s Central European Summer Time
Not Valid After	Wednesday 28 October 2015 13 h 00 min 00 s Central European Standard Time
Public Key Info	
Algorithm	Elliptic Curve Public Key (1.2.840.10045.2.1)
Parameters	Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
Public Key	65 bytes : 04 D8 D1 DD 35 BD E2 59 ...
Key Size	256 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 77 27 91 2D BE AA 22 68 ...
Extension	Key Usage (2.5.29.15)

The ECC standard curve secp256r1

$$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$$

E given by

$$y^2 = x^3 - 3x + b,$$

where

$$\begin{aligned} b =& 41058363725152142129326129780047268409114441015993725554835256314039467401291 \\ G =& (48439561293906451759052585252797914202762949526041747995844080717082404635286, \\ & 36134250956749795798585127919587881956611106672985015071877198253568414405109) \end{aligned}$$

Conclusions

- Geometry exists not only over $\mathbf{R}$, but also over $\mathbf{F}_p$ (integers modulo p).
- https always uses algebra, geometry, number theory for setting up the connection (RSA, Diffie-Hellman, ECC).
- Elliptic curves are used by Google Mail and Facebook.