Diffie-Hellman and Discrete Logarithm computation

Aurore Guillevic

Aarhus University

March 17, 2022

Elliptic Curves, Number Theory and Cryptography, Week 7 These slides at
`https://members.loria.fr/AGuillevic/files/Enseignements/AU/lectures/lecture07B.pdf`

Outline

Lecture notes of another lecture available at
`gitlab.inria.fr/guillevi/enseignement/`

Outline

Discrete logarithm problem

G multiplicative group of order r
g generator, $\mathbf{G} = \{1, g, g^2, g^3, \ldots, g^{r-2}, g^{r-1}\}$

Given $h \in \mathbf{G}$, find integer $x \in \{0, 1, \ldots, r-1\}$ such that $h = g^x$.
Exponentiation easy: $(g, x) \mapsto g^x$
Discrete logarithm hard in well-chosen groups **G**

Choice of group

Prime finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where p is a prime integer
Multiplicative group: $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$
Multiplication *modulo* p

Finite field $\mathbb{F}_{2^n} = \mathrm{GF}(2^n)$, $\mathbb{F}_{3^m} = \mathrm{GF}(3^m)$ for efficient arithmetic, now broken

Elliptic curves $E\colon y^2 = x^3 + ax + b/\mathbb{F}_p$

Diffie-Hellman key exchange

Alice **Bob**

Diffie-Hellman key exchange

Alice

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

public parameters

Bob

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

Diffie-Hellman key exchange

Alice

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

secret key $\mathsf{sk}_A = a \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$

public value $\mathsf{PK}_A = g^a$

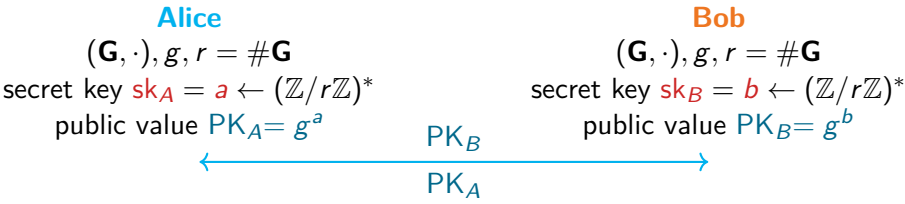
Bob

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

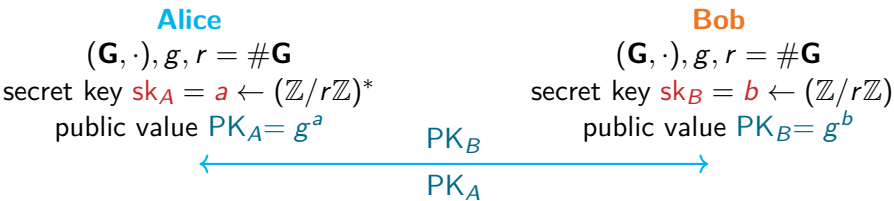
secret key $\mathsf{sk}_B = b \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$

public value $\mathsf{PK}_B = g^b$

Diffie-Hellman key exchange



Diffie-Hellman key exchange



ElGamal, Schnorr signature, DSA

ElGamal encryption

Alice **Bob**

ElGamal encryption

Alice

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

public parameters

Bob

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

ElGamal encryption

Alice

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

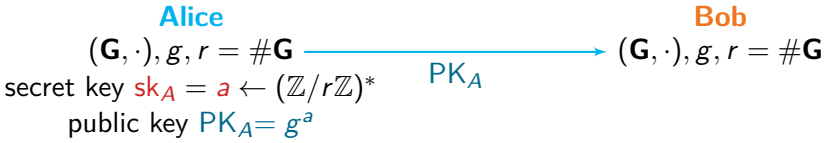
secret key $\mathsf{sk}_A = a \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$

public key $\mathsf{PK}_A = g^a$

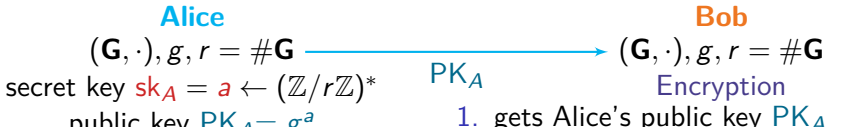
Bob

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

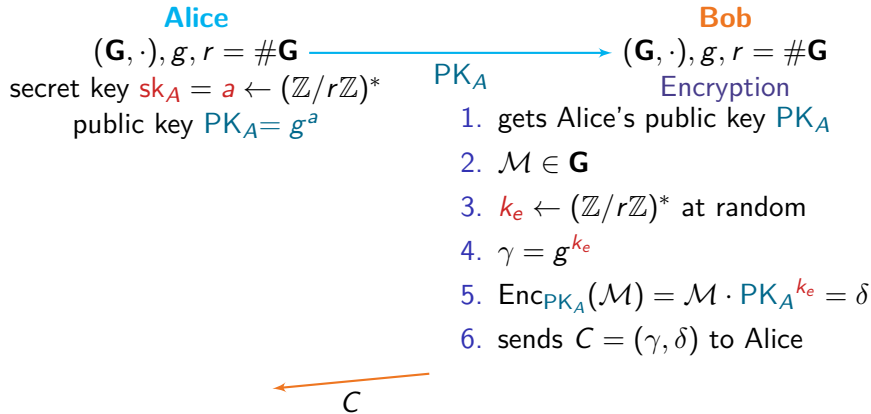
ElGamal encryption



ElGamal encryption



ElGamal encryption



ElGamal encryption

Alice

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

secret key $\mathsf{sk}_A = a \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$

public key $\mathsf{PK}_A = g^a$

PK_A

Bob

$(\mathbf{G}, \cdot), g, r = \#\mathbf{G}$

1. gets Alice's public key PK_A
2. $\mathcal{M} \in \mathbf{G}$
3. $k_e \leftarrow (\mathbb{Z}/r\mathbb{Z})^*$ at random
4. $\gamma = g^{k_e}$
5. $\mathsf{Enc}_{\mathsf{PK}_A}(\mathcal{M}) = \mathcal{M} \cdot {\mathsf{PK}_A}^{k_e} = \delta$
6. sends $C = (\gamma, \delta)$ to Alice

Decryption

C

7. get $C = (\gamma, \delta)$ from Bob
8. $\mathsf{Dec}_{\mathsf{sk}_A}(C) = (\gamma^{-a}) \cdot \delta = \mathcal{M}$

Asymmetric cryptography

Factorization (RSA cryptosystem)

Discrete logarithm problem (use in Diffie-Hellman, etc)

Given a finite cyclic group $(\mathbf{G}, \cdot)$, a generator g and $h \in \mathbf{G}$, compute x s.t. $h = g^x$.
$\rightarrow$ can we invert the exponentiation function $(g, x) \mapsto g^x$?

Common choice of $\mathbf{G}$:

- prime finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (1976)
- characteristic 2 field $\mathbb{F}_{2^n}$ ($\approx$ 1979)
- elliptic curve $E(\mathbb{F}_p)$ (1985)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $g \in G$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#G\}$
- naive search, try them all: $\#G$ tests
- $O(\sqrt{\#G})$ generic algorithms

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $g \in G$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#G\}$
- naive search, try them all: $\#G$ tests
- $O(\sqrt{\#G})$ generic algorithms
  - Shanks baby-step-giant-step (BSGS): $O(\sqrt{\#G})$, deterministic
  - random walk in G, cycle path finding algorithm in a connected graph (Floyd) $\rightarrow$ Pollard: $O(\sqrt{\#G})$, probabilistic
    (the cycle path encodes the answer)
  - parallel search (parallel Pollard, Kangarous)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $g \in G$ generator, $\exists$ always a preimage $x \in \{1, \ldots, \#G\}$
- naive search, try them all: $\#G$ tests
- $O(\sqrt{\#G})$ generic algorithms
  - Shanks baby-step-giant-step (BSGS): $O(\sqrt{\#G})$, deterministic
  - random walk in G, cycle path finding algorithm in a connected graph (Floyd) $\rightarrow$ Pollard: $O(\sqrt{\#G})$, probabilistic
    (the cycle path encodes the answer)
  - parallel search (parallel Pollard, Kangarous)
- independent search in each distinct subgroup
  + Chinese remainder theorem (Pohlig-Hellman)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $\rightarrow$ choose G of large prime order (no subgroup)
- $\rightarrow$ complexity of inverting exponentiation in $O(\sqrt{\#G})$
- $\rightarrow$ security level 128 bits means $\sqrt{\#G} \geq 2^{128}$
  take $\#G = 2^{256}$
  analogy with symmetric crypto, keylength 128 bits (16 bytes)

Discrete log problem

How fast can we invert the exponentiation function $(g, x) \mapsto g^x$?

- $\rightarrow$ choose G of large prime order (no subgroup)
- $\rightarrow$ complexity of inverting exponentiation in $O(\sqrt{\#G})$
- $\rightarrow$ security level 128 bits means $\sqrt{\#G} \geq 2^{128}$
  take $\#G = 2^{256}$
  analogy with symmetric crypto, keylength 128 bits (16 bytes)

Use additional structure of G if any.

Discrete log problem when $\mathbf{G} = (\mathbb{Z}/p\mathbb{Z})^*$

Index calculus algorithm [Western–Miller 68, Adleman 79],
prequel of the Number Field Sieve algorithm (NFS)

- p prime, $(p-1)/2$ prime, $\mathbf{G} = (\mathbb{Z}/p\mathbb{Z})^*$, gen. g, target h
- get many multiplicative relations in $\mathbf{G}$
  $g^t = g_1^{e_1} g_2^{e_2} \cdots g_i^{e_i} \pmod{p}$, $g, g_1, g_2, \ldots, g_i \in \mathbf{G}$
- find a relation $h \cdot g^s = g_1^{e'_1} g_2^{e'_2} \cdots g_i^{e'_i} \pmod{p}$
- take logarithm: linear relations

$$\begin{aligned} t &= e_1 \log g_1 + e_2 \log g_2 + \ldots + e_i \log g_i \pmod{p-1} \\ &\vdots \\ \log h &= -s + e'_1 \log g_1 + e'_2 \log g_2 + \ldots + e'_i \log g_i \pmod{p-1} \end{aligned}$$

- solve a linear system
- get $x = \log h$

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$: example

$p = 1109$, $r = (p-1)/4 = 277$ prime
Smoothness bound $B = 13$
$\mathcal{F}_{13} = \{2, 3, 5, 7, 11, 13\}$ small primes up to B, $i = \#\mathcal{F}$
B-smooth integer: $n = \prod_{p_i \le B} p_i^{e_i}$, p_i prime
is g^s smooth? $1 \le s \le 72$ is enough

$$
\begin{array}{ll}
g^{1} = & 2 = 2 \\
g^{13} = & 429 = 3 \cdot 11 \cdot 13 \\
g^{16} = & 105 = 3 \cdot 5 \cdot 7 \\
g^{21} = & 33 = 3 \cdot 11 \\
g^{44} = & 1029 = 3 \cdot 7^3 \\
g^{72} = & 325 = 5^2 \cdot 13
\end{array}
\quad \rightarrow \quad
\begin{array}{c}
\begin{matrix} 2 & 3 & 5 & 7 & 11 & 13 \end{matrix} \\
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 3 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 1
\end{bmatrix}
\end{array}
\cdot \vec{x} =
\begin{bmatrix}
1 \\ 13 \\ 16 \\ 21 \\ 44 \\ 72
\end{bmatrix}
$$

$\vec{x} = [1, 219, 40, 34, 79, 269] \bmod 277$

$\rightarrow \log_g 7 = 34 \bmod 277$, that is, $(g^{34})^4 = 7^4$
$g^{34} = 7u$ and $u^4 = 1$

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$: example

$\vec{x} = [1, 219, 40, 34, 79, 269] \bmod 277$
subgroup of order 4: $g_4 = g^{(p-1)/4}$
$\{1, g_4, g_4^2, g_4^3\} = \{1, 354, 1108, 755\}$

Pohlig-Hellman:

$$
\begin{aligned}
3/g^{219} &= 1 = 1 \Rightarrow \log_g 3 &&= 219 \\
5/g^{40} &= 1108 = -1 \Rightarrow \log_g 5 &&= 40 + (p-1)/2 = 594 \\
7/g^{34} &= 354 = g_4 \Rightarrow \log_g 7 &&= 34 + (p-1)/4 = 311 \\
11/g^{79} &= 755 = g_4^3 \Rightarrow \log_g 11 &&= 79 + 3(p-1)/4 = 910 \\
13/g^{269} &= 755 = g_4^3 \Rightarrow \log_g 13 &&= 269 + 3(p-1)/4 = 1100
\end{aligned}
$$

$\vec{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$

Target $h = 777$
$g^{10} \cdot 777 = 495 = 3^2 \cdot 5 \cdot 11 \bmod p$
$\log_2 777 = -10 + 2\log_g 3 + \log_g 5 + \log_g 11 = 824 \bmod p - 1$
$g^{824} = 777$

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$: example

Trick

Multiplicative relations over the **integers**

$g_1, g_2, \ldots, g_i \longleftrightarrow$ small prime integers

Smooth integers $n = \prod_{p_i \leq B} p_i^{e_i}$ are quite common $\rightarrow$ it works

Complexity $e^{\sqrt{(2+o(1))(\log p)(\log\log p)}}$ (Pomerance 87)

Index calculus in $(\mathbb{Z}/p\mathbb{Z})^*$: example

Trick

Multiplicative relations over the **integers**

$g_1, g_2, \ldots, g_i \longleftrightarrow$ small prime integers

Smooth integers $n = \prod_{p_i \leq B} p_i^{e_i}$ are quite common $\rightarrow$ it works

Complexity $e^{\sqrt{(2+o(1))(\log p)(\log\log p)}}$ (Pomerance 87)

Improvements in the 80's, 90's:

- Sieve (faster relation collection)
- Smaller integers to factor
- Multiplicative relations in **number fields**
- Better **sparse linear algebra**
- Independent targets h

Number Field: Toy example with $\mathbb{Z}[i]$

1986: Coppersmith–Odlyzko–Schroeppel, DL in GF(p)

If $p = 1 \bmod 4$, $\exists\ U, V$ s.t. $p = U^2 + V^2$
and $|U|, |V| < \sqrt{p}$
$U/V \equiv m \mod p$ and $m^2 + 1 = 0 \mod p$

Define a map from $\mathbb{Z}[i]$ to $\mathbb{Z}/p\mathbb{Z}$

$$\begin{array}{rcl} \phi\colon \mathbb{Z}[i] & \to & \mathbb{Z}/p\mathbb{Z} \\ i & \mapsto & m \bmod p \text{ where } m = U/V,\ m^2 + 1 = 0 \bmod p \end{array}$$

ring homomorphism $\phi(a + bi) = a + bm$

$$\phi(\underbrace{a + bi}_{\text{factor in } \mathbb{Z}[i]}) = a + bm = (a + b\ \underbrace{U/V}_{=m}) = (\underbrace{aV + bU}_{\text{factor in } \mathbb{Z}})V^{-1} \mod p$$

Example in $\mathbb{Z}[i]$

$p = 1109 = 1 \bmod 4$, $r = (p-1)/4 = 277$ prime
$p = 22^2 + 25^2$
$\max(|a|, |b|) = A = 20$, $B = 13$ smoothness bound

Example in $\mathbb{Z}[i]$

$p = 1109 = 1 \bmod 4$, $r = (p-1)/4 = 277$ prime
$p = 22^2 + 25^2$
$\max(|a|, |b|) = A = 20$, $B = 13$ smoothness bound

Rational side

$\mathcal{F}_{\text{rat}} = \{2, 3, 5, 7, 11, 13\}$ primes up to B
$g(x) = Vx - U$

Example in $\mathbb{Z}[i]$

$p = 1109 = 1 \bmod 4$, $r = (p-1)/4 = 277$ prime
$p = 22^2 + 25^2$
$\max(|a|, |b|) = A = 20$, $B = 13$ smoothness bound

Rational side

$\mathcal{F}_{\text{rat}} = \{2, 3, 5, 7, 11, 13\}$ primes up to B
$g(x) = Vx - U$

Algebraic side: think about the complex number in $\mathbb{C}$

$-i(1+i)^2 = 2$, $(2+i)(2-i) = 5$, $(2+3i)(2-3i) = 13$
$\mathcal{F}_{\text{alg}} = \{1+i, 2+i, 2-i, 2+3i, 2-3i\}$
"primes" of norm up to B
$f(x) = x^2 + 1$

Example in $\mathbb{Z}[i]$

$p = 1109 = 1 \bmod 4$, $r = (p-1)/4 = 277$ prime
$p = 22^2 + 25^2$
$\max(|a|, |b|) = A = 20$, $B = 13$ smoothness bound

Rational side

$\mathcal{F}_{\text{rat}} = \{2, 3, 5, 7, 11, 13\}$ primes up to B
$g(x) = Vx - U$

Algebraic side: think about the complex number in $\mathbb{C}$

$-i(1+i)^2 = 2$, $(2+i)(2-i) = 5$, $(2+3i)(2-3i) = 13$
$\mathcal{F}_{\text{alg}} = \{1+i, 2+i, 2-i, 2+3i, 2-3i\}$
"primes" of norm up to B
$f(x) = x^2 + 1$

Units

$\mathcal{U}_{\text{alg}} = \{-1, i, -i\}$

Example in $\mathbb{Z}[i]$

$p = 1109$

$(a, b) = (-4, 7)$,
$\text{Norm}(-4 + 7i) = (-4)^2 + 7^2 = 65 = 5 \cdot 13$

In $\mathbb{Z}[i]$,

- $5 = (2 + i)(2 - i)$
- $13 = (2 + 3i)(2 - 3i)$

Example in $\mathbb{Z}[i]$

$p = 1109$

$(a, b) = (-4, 7)$,
$\text{Norm}(-4 + 7i) = (-4)^2 + 7^2 = 65 = 5 \cdot 13$

In $\mathbb{Z}[i]$,

- $5 = (2 + i)(2 - i)$
- $13 = (2 + 3i)(2 - 3i)$

$\rightarrow$ $(2 \pm i)(2 \pm 3i)$ has norm 65

$\rightarrow$ $\pm i(2 \pm i)(2 \pm 3i) = (-4 + 7i)$

We obtain $i(2 - i)(2 + 3i) = -4 + 7i$

Example in $\mathbb{Z}[i]$

$p = 1109$

$(a, b) = (-4, 7)$,
$\text{Norm}(-4 + 7i) = (-4)^2 + 7^2 = 65 = 5 \cdot 13$

In $\mathbb{Z}[i]$,

- $5 = (2 + i)(2 - i)$
- $13 = (2 + 3i)(2 - 3i)$

$\rightarrow$ $(2 \pm i)(2 \pm 3i)$ has norm 65

$\rightarrow$ $\pm i(2 \pm i)(2 \pm 3i) = (-4 + 7i)$

We obtain $i(2 - i)(2 + 3i) = -4 + 7i$

$i \leftrightarrow m = 22/25 = 755 \bmod p$
$m(2 - m)(2 + 3m) = 845 \bmod p$
$-4 + 7m = 845 \bmod p$
$(-4 \cdot 25 + 7 \cdot 22)/25 = 845 \bmod p$

Example in $\mathbb{Z}[i]$

$a+bi$	$aV+bU=$ factor in $\mathbb{Z}$	a^2+b^2	factor in $\mathbb{Z}[i]$
$-17+19i$	$-7=-7$	$650=2\cdot 5^2\cdot 13$	$i(1+i)(2+i)^2(2-3i)$
$-11+2i$	$-231=-3\cdot 7\cdot 11$	$125=5^3$	$i(2+i)^3$
$-6+17i$	$224=2^5\cdot 7$	$325=5^2\cdot 13$	$(2+i)^2(2+3i)$
$-4+7i$	$54=2\cdot 3^3$	$65=5\cdot 13$	$i(2-i)(2+3i)$
$-3+4i$	$13=13$	$25=5^2$	$-(2-i)^2$
$-2+i$	$-28=-2^2\cdot 7$	$5=5$	$-(2-i)$
$-2+3i$	$16=2^4$	$13=13$	$-(2-3i)$
$-2+11i$	$192=2^6\cdot 3$	$125=5^3$	$-(2-i)^3$
$-1+i$	$-3=-3$	$2=2$	$i(1+i)$
i	$22=2\cdot 11$	$1=1$	i
$1+3i$	$91=7\cdot 13$	$10=2\cdot 5$	$(1+i)(2+i)$
$1+5i$	$135=3^3\cdot 5$	$26=2\cdot 13$	$i(1+i)(2-3i)$
$2+i$	$72=2^3\cdot 3^2$	$5=5$	$(2+i)$
$5+i$	$147=3\cdot 7^2$	$26=2\cdot 13$	$-i(1+i)(2+3i)$

Example in $\mathbb{Z}[i]$: Matrix

Build the matrix of relations:

- one row per (a, b) pair s.t. both norms are smooth
- one column per prime of $\mathcal{F}_{\text{rat}}$
- one column for $1/V$
- one column per prime ideal of $\mathcal{F}_{\text{alg}}$
- one column per unit $(-1, i)$
- store the exponents

$$
M = \begin{array}{c}
\begin{array}{cccccccccccccc}
2 & 3 & 5 & 7 & 11 & 13 & \frac{1}{V} & -1 & i & 1+i & 2+i & 2-i & 2+3i & 2-3i
\end{array} \\
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 3 & 0 & 0 & 0 \\
5 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \\
1 & 3 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 2 & 0 & 0 \\
2 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
4 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
6 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 3 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 3 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
3 & 2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 2 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0
\end{bmatrix}
\end{array}
$$

$$
M = \begin{array}{c}
\begin{array}{cccccccccccccc}
2 & 3 & 5 & 7 & 11 & 13 & \frac{1}{V} & -1 & i & 1+i & 2+i & 2-i & 2+3i & 2-3i
\end{array} \\
\left[\begin{array}{cccccccccccccc}
 & & & & & & & 1 & 2 & & & & & \\
 & & & 1 & & & 1 & 1 & 1 & 1 & 2 & & & 1 \\
 & 1 & & 1 & 1 & & 1 & 1 & 1 & & 3 & & & \\
5 & & & 1 & & & 1 & & & & 2 & & 1 & \\
1 & 3 & & & & & 1 & & 1 & & & 1 & 1 & \\
 & & & & & 1 & 1 & 1 & & & & 2 & & \\
2 & & & 1 & & & 1 & & & & & 1 & & \\
4 & & & & & & 1 & 1 & & & & & & 1 \\
6 & 1 & & & & & 1 & 1 & & & & 3 & & \\
 & 1 & & & & & 1 & 1 & 1 & 1 & & & & \\
1 & & & & 1 & & 1 & & 1 & & & & & \\
 & & & 1 & & 1 & 1 & & & 1 & 1 & & & \\
 & 3 & 1 & & & & 1 & & 1 & 1 & & & & 1 \\
3 & 2 & & & & & 1 & & & & 1 & & & \\
 & 1 & & 2 & & & 1 & 1 & 1 & 1 & & & 1 &
\end{array}\right]
\end{array}
$$

$$
M = \begin{array}{c}
\begin{array}{cccccccccccccc}
2 & 3 & 5 & 7 & 11 & 13 & \frac{1}{V} & -1 & i & 1+i & 2+i & 2-i & 2+3i & 2-3i
\end{array} \\
\left[\begin{array}{cccccccccccccc}
 & & & & & & & -1 & -2 & & & & & \\
 & & & 1 & & & 1 & -1 & -1 & -1 & -2 & & & -1 \\
 & 1 & & 1 & 1 & & 1 & -1 & -1 & & -3 & & & \\
5 & & & 1 & & & 1 & & & & -2 & & -1 & \\
1 & 3 & & & & & 1 & & -1 & & & -1 & -1 & \\
 & & & & & 1 & 1 & -1 & & & & -2 & & \\
2 & & & 1 & & & 1 & & & & & -1 & & \\
4 & & & & & & 1 & -1 & & & & & & -1 \\
6 & 1 & & & & & 1 & -1 & & & & -3 & & \\
 & 1 & & & & & 1 & -1 & -1 & -1 & & & & \\
1 & & & & 1 & & 1 & & -1 & & & & & \\
 & & & 1 & & 1 & 1 & & & -1 & -1 & & & \\
 & 3 & 1 & & & & 1 & & -1 & -1 & & & & -1 \\
3 & 2 & & & & & 1 & & & & -1 & & & \\
 & 1 & & 2 & & & 1 & -1 & -1 & -1 & & & -1 &
\end{array}\right]
\end{array}
$$

Example in $\mathbb{Z}[i]$

Right kernel $M \cdot \vec{x} = 0 \bmod (p-1)/4 = 277$:

$$\vec{x} = (\underbrace{1, 219, 40, 34, 79, 269}_{\text{rational side}}, \underbrace{197}_{1/V}, \underbrace{0, 0}_{\text{units}}, \underbrace{139, 84, 233, 68, 201}_{\text{algebraic side}})$$

Logarithms (in some basis)

Example in $\mathbb{Z}[i]$

Right kernel $M \cdot \vec{x} = 0 \bmod (p-1)/4 = 277$:

$$\vec{x} = (\underbrace{1, 219, 40, 34, 79, 269}_{\text{rational side}}, \underbrace{197}_{1/V}, \underbrace{0, 0}_{\text{units}}, \underbrace{139, 84, 233, 68, 201}_{\text{algebraic side}})$$

Logarithms (in some basis)

Rational side: logarithms of $\{2, 3, 5, 7, 11, 13\}$ in basis 2

$\vec{x} = [1, 219, 40, 34, 79, 269] \bmod 277$

$\rightarrow$ order 4 subgroup

$\vec{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$

Example in $\mathbb{Z}[i]$

Right kernel $M \cdot \vec{x} = 0 \bmod (p-1)/4 = 277$:

$$\vec{x} = (\underbrace{1, 219, 40, 34, 79, 269}_{\text{rational side}}, \underbrace{197}_{1/V}, \underbrace{0, 0}_{\text{units}}, \underbrace{139, 84, 233, 68, 201}_{\text{algebraic side}})$$

Logarithms (in some basis)

Rational side: logarithms of $\{2, 3, 5, 7, 11, 13\}$ in basis 2

$\vec{x} = [1, 219, 40, 34, 79, 269] \bmod 277$

$\rightarrow$ order 4 subgroup

$\vec{v} = [1, 219, 594, 311, 910, 1100] \bmod p - 1$

Target 314, generator $g = 2$

$314 = -20/7 \bmod p = -2^2 \cdot 5/7$

$$\begin{aligned} \log_g 314 &= \log_g -1 + 2\log_g 2 + \log_g 5 - \log_g 7 \\ &= (p-1)/2 + 2 + 594 - 311 = 839 \bmod p - 1 \end{aligned}$$

$2^{839} = 314 \bmod p$

Number Field Sieve

Since 1993 (Gordon, Schirokauer):

$$L_p(1/3, c) = e^{(c+o(1))(\log p)^{1/3}(\log\log p)^{2/3}}$$

- polynomial selection
- **relation collection** $L_p(1/3, 1.923)$
  sieve to enumerate efficiently (a, b) pairs
- **sparse linear algebra** $L_p(1/3, 1.923)$
  compute right kernel mod prime ℓ, block-Wiedemann alg.
- individual discrete logarithm

Outline

Attacks on discrete-logarithm based cryptosystems

1. Sony Play-Station 3 (PS3) hacking
   1.1 ECDSA signature
   1.2 PS3 problem
2. Weak DH attack
3. Weak keys in the Moscow internet voting system

Sony Play-Station 3 (PS3) hacking

A problem of bad randomness in the ECDSA signature.
Slides of the talk at CCC 122-134:
`https://fahrplan.events.ccc.de/congress/2010/Fahrplan/attachments/1780_27c3_console_hacking_2010.pdf`
Chaos Communication Congress, every year in Germany

The same random token was used to sign everything.
$\rightarrow$ With two public signatures,
one can recover the private key and then sign anything with this private key.

ECDSA signature

(From textbook Paar Pelzl, Chapter 10 section 5)

ECDSA: Elliptic Curve Digital Signature Algorithm

needs an elliptic curve E defined over a prime field $\mathbb{F}_p$
(works also for curves defined over other fields such as $\mathbb{F}_{2^n}$)
Assume $E(\mathbb{F}_p)$ has a subgroup of large prime order q
$G(x_G, y_G)$ is a generator

Public Parameters

- p
- Elliptic curve E (coefficients of the curve equation)
- group order q (prime)
- generator of order q: $G(x_G, y_G)$

ECDSA signature

Key generation

1. Choose a random integer d in $\{1, \ldots, q-1\}$
2. Compute the point $P = d \cdot G$
3. Public key: $(p, q, E$ (coefficients), $G, P)$
4. Private key: (d)

H is a cryptographic hash function whose output is at least of the same length as of q (for example, 256 bits or 32 bytes)

ECDSA signature

Signing of a message m

1. Choose an ephemeral private key as an integer k_e in $\{1, \ldots, q-1\}$
2. Compute the point $R = k_e \cdot G$
3. Let $r = x_R$ the x-coordinate of the point R.
4. Compute $s = (H(m) + d \cdot r) \cdot k_e^{-1} \bmod q$. The signature is (r, s).

Verification

1. Compute $w = s^{-1} \bmod q$
2. Compute $u_1 = w \cdot H(m) \bmod q$ (with the same hash function H)
3. Compute $u_2 = w \cdot r \bmod q$
4. Compute $Q = u_1 \cdot G + u_2 \cdot P$ (a point on E)
5. if $x_Q = r \bmod q$ then the signature is valid, otherwise the signature is invalid.

PS3 problem

The hackers discovered that the same ephemeral key k_e was used to sign different things.

$\rightarrow$ collect the data for distinct messages, say m_1 and m_2.

- $(r, s_1 = (H(m_1) + d \cdot r) \cdot k_e^{-1} \bmod q$
- $(r, s_2 = (H(m_2) + d \cdot r) \cdot k_e^{-1} \bmod q$

One wants to recover the private key d. Observe that

$$\begin{aligned} s_1 - s_2 \bmod q &= (H(m_1) + d \cdot r) \cdot k_e^{-1} - (H(m_2) + d \cdot r) \cdot k_e^{-1} \\ &= (H(m_1) - H(m_2)) \cdot k_e^{-1} \bmod q \end{aligned}$$

The secret key d vanished! We can publicly compute $h = H(m_1) - H(m_2) \bmod q$, then recover the (actually non-ephemeral) key k_e.

PS3 problem

$$h = H(m_1) - H(m_2) \bmod q$$
$$k_e = h/(s_1 - s_2) \bmod q$$
$$d = (s_1 \cdot k_e - H(m_1))/r \bmod q$$

Knowing the manufacturer's private key d allows to sign non-legitimate documents (software, games for the PS3), and the signature will be accepted as a valid signature by any verifier.

Weak DH attack

https://weakdh.org/
https://weakdh.org/weakdh-ccs-slides.pdf

Weak keys in the Moscow internet voting system

https://members.loria.fr/PGaudry/moscow/
https://hal.inria.fr/hal-02266264v2
https://rwc.iacr.org/2020/slides/Gaudry.pdf

Discrete logarithm computation in finite fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{3^m}$

GF(2^{30750}) in 2019 by Granger, Kleinjung, Lenstra, Wesolowski and Zumbrägel