Probabilistic Algorithms Related to RSA

FA 2018 Cryptography Seminar

J. David Taylor

October 19, 2018

Discrete Logarithm Problem

Let g be a primitive root mod p and let $h \in \mathbb{F}_p^*$.

Discrete Logarithm Problem

Let g be a primitive root mod p and let $h \in \mathbb{F}_p^*$.

The solution of the congruence

$$g^x \equiv h \mod p$$

is called $\log(h)$ and is defined mod $p - 1$.

Discrete Logarithm Problem

Let g be a primitive root mod p and let $h \in \mathbb{F}_p^*$.

The solution of the congruence

$$g^x \equiv h \mod p$$

is called $\log(h)$ and is defined mod $p - 1$.

Note that it depends on g.

Breaking up the DLP

Instead of solving

$$g^x \equiv h \mod p,$$

Breaking up the DLP

Instead of solving

$$g^x \equiv h \mod p,$$

we can try solving

$$g^x \equiv h \mod \ell$$

for all B-smooth primes ℓ.

Reduction to B-smooth primes

We will compute $h \cdot g^{-k} \mod p$ for $k \geq 1$ until we hit a B-smooth residue.

Reduction to B-smooth primes

We will compute $h \cdot g^{-k} \mod p$ for $k \geq 1$ until we hit a B-smooth residue.

The factorization

$$h \cdot g^{-k} = \prod_{\ell \leq B} \ell^{e_\ell}$$

implies that

$$\log(h) \equiv k + \sum_{\ell \leq B} e_\ell \log(\ell) \mod p - 1$$

Reduction to B-smooth primes

We will compute $h \cdot g^{-k} \mod p$ for $k \geq 1$ until we hit a B-smooth residue.

The factorization

$$h \cdot g^{-k} = \prod_{\ell \leq B} \ell^{e_\ell}$$

implies that

$$\log(h) \equiv k + \sum_{\ell \leq B} e_\ell \log(\ell) \mod p - 1$$

Now we need a method to calculate $\log(\ell)$ for all B-smooth primes ℓ.

Finding $\log(\ell)$

1. Pick random $i \in \{1, \ldots, p-1\}$.

Finding $\log(\ell)$

1. Pick random $i \in \{1, \ldots, p-1\}$.
2. Define g_i as the least positive residue of $g^i \mod p$.

Finding $\log(\ell)$

1. Pick random $i \in \{1, \ldots, p-1\}$.
2. Define g_i as the least positive residue of $g^i \mod p$.
3. Keep g_i, if it is B-smooth.

Finding $\log(\ell)$

1. Pick random $i \in \{1, \ldots, p-1\}$.
2. Define g_i as the least positive residue of $g^i \mod p$.
3. Keep g_i, if it is B-smooth.
4. Factor $g_i = \prod_{\ell \leq B} \ell^{u_\ell(i)}$

Finding $\log(\ell)$

1. Pick random $i \in \{1, \ldots, p-1\}$.
2. Define g_i as the least positive residue of $g^i \mod p$.
3. Keep g_i, if it is B-smooth.
4. Factor $g_i = \prod_{\ell \leq B} \ell^{u_\ell(i)}$

Note that

$$i \equiv \sum_{\ell \leq B} u_\ell(i) \log(\ell) \mod p-1.$$

Finding $\log(\ell)$

1. Pick random $i \in \{1, \ldots, p-1\}$.
2. Define g_i as the least positive residue of $g^i \mod p$.
3. Keep g_i, if it is B-smooth.
4. Factor $g_i = \prod_{\ell \leq B} \ell^{u_\ell(i)}$

Note that

$$i \equiv \sum_{\ell \leq B} u_\ell(i) \log(\ell) \mod p-1.$$

Get more than $\pi(B)$-equations for an overdetermined system mod $p-1$.

Finding $\log(\ell)$

1. Pick random $i \in \{1, \ldots, p-1\}$.
2. Define g_i as the least positive residue of $g^i \mod p$.
3. Keep g_i, if it is B-smooth.
4. Factor $g_i = \prod_{\ell \leq B} \ell^{u_\ell(i)}$

Note that

$$i \equiv \sum_{\ell \leq B} u_\ell(i) \log(\ell) \mod p-1.$$

Get more than $\pi(B)$-equations for an overdetermined system mod $p-1$.

Use the Chinese remainder theorem to solve the resulting system.

Index Calculus Example (Taken from HPS)

Let's solve

$$37^x \equiv 211 \mod 18443.$$

Index Calculus Example (Taken from HPS)

Let's solve

$$37^x \equiv 211 \mod 18443.$$

Note that $p = 18443$ is a prime with primitive root $g = 37$.

Index Calculus Example (Taken from HPS)

Let's solve

$$37^x \equiv 211 \mod 18443.$$

Note that $p = 18443$ is a prime with primitive root $g = 37$.

Take $B = 5$, so the smooth primes are 2, 3, 5.

Index Calculus Example (Taken from HPS)

Pick random powers to get

$$g^{12708} \equiv 2^3 \cdot 3^4 \cdot 5 \mod p, \quad g^{11311} \equiv 2^3 \cdot 5^2 \mod p$$

$$g^{15400} \equiv 2^3 \cdot 3^3 \cdot 5 \mod p, \quad g^{2731} \equiv 2^3 \cdot 3 \cdot 5^4 \mod p$$

Index Calculus Example (Taken from HPS)

Pick random powers to get

$$g^{12708} \equiv 2^3 \cdot 3^4 \cdot 5 \mod p, \quad g^{11311} \equiv 2^3 \cdot 5^2 \mod p$$
$$g^{15400} \equiv 2^3 \cdot 3^3 \cdot 5 \mod p, \quad g^{2731} \equiv 2^3 \cdot 3 \cdot 5^4 \mod p$$

Convert this to the linear system $\mod p-1$:

$$\begin{aligned} 12708 &\equiv 3x_2 + 4x_3 + x_5 \\ 11311 &\equiv 3x_2 + 0x_3 + 2x_5 \\ 15400 &\equiv 3x_2 + 3x_3 + x_5 \\ 2731 &\equiv 3x_2 + x_3 + 4x_5 \end{aligned}$$

Index Calculus Example (Taken from HPS)

Note that $p - 1 = 18442 = 2 \cdot 9221$.

Index Calculus Example (Taken from HPS)

Note that $p - 1 = 18442 = 2 \cdot 9221$.

Gaussian elimination yields solutions

$$(1, 0, 1) \mod 2 \text{ and } (5733, 6529, 6277) \mod 9221.$$

Index Calculus Example (Taken from HPS)

Note that $p - 1 = 18442 = 2 \cdot 9221$.

Gaussian elimination yields solutions

$$(1, 0, 1) \mod 2 \text{ and } (5733, 6529, 6277) \mod 9221.$$

These combine to give $\mod p - 1$:

$$\log(2) \equiv 5733$$
$$\log(3) \equiv 15750$$
$$\log(5) \equiv 6277$$

Index Calculus Example (Taken from HPS)

We want to solve

$$37^x \equiv 211 \mod 18443.$$

Index Calculus Example (Taken from HPS)

We want to solve

$$37^x \equiv 211 \mod 18443.$$

Compute residues of $211 \cdot 37^{-k} \mod 18443$ until we find one that is 5-smooth (choose k at random).

Index Calculus Example (Taken from HPS)

We want to solve

$$37^x \equiv 211 \mod 18443.$$

Compute residues of $211 \cdot 37^{-k} \mod 18443$ until we find one that is 5-smooth (choose k at random).

We find that

$$211 \cdot 37^{-9549} \equiv 2^5 \cdot 3^2 \cdot 5^2 \mod 18443.$$

Index Calculus Example (Taken from HPS)

Putting this all together $\mod 18442$:

$$\begin{aligned}\log(211) &\equiv 9549 + 5\log(2) + 2\log(3) + 2\log(5) \\ &\equiv 8500\end{aligned}$$

Index Calculus Runtime

The Index Calculus has a subexponential runtime of $\mathcal{O}\left(L_p[1/2, \sqrt{2}]\right)$, where

$$L_p[1/2, \sqrt{2}] = \exp\left((\sqrt{2} + o(1))(\log p)^{1/2}(\log\log p)^{1/2}\right).$$

Index Calculus Runtime

The Index Calculus has a subexponential runtime of $\mathcal{O}\left(L_p[1/2, \sqrt{2}]\right)$, where

$$L_p[1/2, \sqrt{2}] = \exp\left((\sqrt{2} + o(1))(\log p)^{1/2}(\log\log p)^{1/2}\right).$$

More generally,

$$L_n[\alpha, c] = e^{(c+o(1))(\log n)^{\alpha}(\log\log n)^{1-\alpha}}$$

is "L-notation".

Index Calculus Runtime

The Index Calculus has a subexponential runtime of $\mathcal{O}\left(L_p[1/2, \sqrt{2}]\right)$, where

$$L_p[1/2, \sqrt{2}] = \exp\left((\sqrt{2} + o(1))(\log p)^{1/2}(\log\log p)^{1/2}\right).$$

More generally,

$$L_n[\alpha, c] = e^{(c+o(1))(\log n)^{\alpha}(\log\log n)^{1-\alpha}}$$

is "L-notation".

If $\alpha = 1$, then L is exponential. $L_n[1, c] = n^{c+o(1)}$
If $\alpha = 0$, then L is polynomial. $L_n[0, c] = (\log n)^{c+o(1)}$

The Problem

The following problem is hard:

"Let a, N be integers. Determine if a is a square mod N."

The Problem

The following problem is hard:

"Let a, N be integers. Determine if a is a square mod N."

The following problem is easy:

"Let p, q be prime numbers and let a be an integer. Determine if a is a square mod pq."

The Problem

The following problem is hard:

"Let a, N be integers. Determine if a is a square mod N."

The following problem is easy:

"Let p, q be prime numbers and let a be an integer. Determine if a is a square mod pq."

Goldwasser and Micali used this dichotomy for their cryptographic scheme.

Quadratic Residues

Let p be a prime number and let a be an integer prime to p.

Quadratic Residues

Let p be a prime number and let a be an integer prime to p.

We say that a is a quadratic residue mod p iff a is a square mod p.

Quadratic Residues

Let p be a prime number and let a be an integer prime to p.

We say that a is a quadratic residue mod p iff a is a square mod p.

We say that a is a quadratic non-residue mod p iff a is not a square mod p.

Quadratic Residues

Let p be a prime number and let a be an integer prime to p.

We say that a is a quadratic residue mod p iff a is a square mod p.

We say that a is a quadratic non-residue mod p iff a is not a square mod p.

Quadratic residues and non-residues multiply with standard parity (e.g. like sums of even or odd numbers).

The Legendre Symbol

The Legendre Symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{otherwise} \end{cases}$$

The Legendre Symbol

The Legendre Symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{otherwise} \end{cases}$$

The Legendre symbol is multiplicative:

$$\text{if } \gcd(m,n) = 1, \text{ then } \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right).$$

Quadratic Reciprocity

Let p, q be an odd primes. Here is the Law of Quadratic Reciprocity:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

Quadratic Reciprocity

Let p, q be an odd primes. Here is the Law of Quadratic Reciprocity:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \mod 8 \\ -1 & \text{if } p \equiv 3, 5 \mod 8 \end{cases}$$

Quadratic Reciprocity

Let p, q be an odd primes. Here is the Law of Quadratic Reciprocity:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \mod 8 \\ -1 & \text{if } p \equiv 3, 5 \mod 8 \end{cases}$$

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \\ -\left(\frac{q}{p}\right) & \text{otherwise} \end{cases}$$

Quadratic Reciprocity

Let p, q be an odd primes. Here is the Law of Quadratic Reciprocity:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \mod 8 \\ -1 & \text{if } p \equiv 3, 5 \mod 8 \end{cases}$$

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \\ -\left(\frac{q}{p}\right) & \text{otherwise} \end{cases}$$

Quadratic Reciprocity Example

Here's an example of Quadratic Reciprocity in Practice:

$$\begin{aligned}
\left(\frac{-15750}{37907}\right) &= \left(\frac{-1}{37907}\right)\left(\frac{15750}{37907}\right) \\
&= (-1)\left(\frac{2 \cdot 3^2 \cdot 5^3 \cdot 7}{37907}\right) \\
&= -\left(\frac{2}{37907}\right)\left(\frac{5}{37907}\right)\left(\frac{7}{37907}\right) \\
&= (-1)^2\left(\frac{37907}{5}\right)(-1)\left(\frac{37907}{7}\right) \\
&= -\left(\frac{2}{5}\right)\left(\frac{2}{7}\right) \\
&= (-1)(-1)(1) \\
&= 1
\end{aligned}$$

Jacobi Symbol

Let a, b be integers with b odd an positive.

Jacobi Symbol

Let a, b be integers with b odd an positive.

Let $b = \prod p^{e_p}$ be the prime factorization of b.

Jacobi Symbol

Let a, b be integers with b odd an positive.

Let $b = \prod p^{e_p}$ be the prime factorization of b.

Define

$$\left(\frac{a}{b}\right) := \prod \left(\frac{a}{p}\right)^{e_p}.$$

This is called the Jacobi symbol.

Jacobi Symbol

Let a, b be integers with b odd an positive.

Let $b = \prod p^{e_p}$ be the prime factorization of b.

Define

$$\left(\frac{a}{b}\right) := \prod \left(\frac{a}{p}\right)^{e_p}.$$

This is called the Jacobi symbol.

It is multiplicative in each coordinate.

Jacobi Symbol

Let a, b be integers with b odd an positive.

Let $b = \prod p^{e_p}$ be the prime factorization of b.

Define

$$\left(\frac{a}{b}\right) := \prod \left(\frac{a}{p}\right)^{e_p}.$$

This is called the Jacobi symbol.

It is multiplicative in each coordinate.

It can detect some quadratic non-residues, but it doesn't give certainty of residues.

Jacobi Symbol

Let a, b be integers with b odd an positive.

Let $b = \prod p^{e_p}$ be the prime factorization of b.

Define

$$\left(\frac{a}{b}\right) := \prod \left(\frac{a}{p}\right)^{e_p}.$$

This is called the Jacobi symbol.

It is multiplicative in each coordinate.

It can detect some quadratic non-residues, but it doesn't give certainty of residues.

For example:

$$\left(\frac{6}{77}\right) = 1$$

but 6 is not a square mod 77.

Key Creation

Bob chooses secret primes p, q.

Key Creation

Bob chooses secret primes p, q.

Bob also chooses an integer a that is a quadratic non-residue modulo each prime.

Key Creation

Bob chooses secret primes p, q.

Bob also chooses an integer a that is a quadratic non-residue modulo each prime.

The public key is $N = pq$ and a.

Encryption

Alice chooses a plaintext $m \in \{0, 1\}$.

Encryption

Alice chooses a plaintext $m \in \{0, 1\}$.

Choose random integer r between 1 and N.

Encryption

Alice chooses a plaintext $m \in \{0, 1\}$.

Choose random integer r between 1 and N.

Compute

$$c := \begin{cases} r^2 \mod N & \text{if } m = 0 \\ ar^2 \mod N & \text{if } m = 1 \end{cases}$$

Encryption

Alice chooses a plaintext $m \in \{0, 1\}$.

Choose random integer r between 1 and N.

Compute

$$c := \begin{cases} r^2 \mod N & \text{if } m = 0 \\ ar^2 \mod N & \text{if } m = 1 \end{cases}$$

Send c to Bob.

Decryption

Bob computes

$$m = \begin{cases} 0 & \text{if } \left(\frac{c}{p}\right) = 1 \\ 1 & \text{if } \left(\frac{c}{p}\right) = -1 \end{cases}$$

Goldwasser-Micali Example

Next time?