Elliptic Curve Cryptography

Joseph Kirtland

Meeting of the Poughkeepsie Chapter of the ACM
Marist College
September 25, 2017
Terminology

plaintext - original message

ciphertext - coded form of the message

enciphering/encryption - converting the plaintext to ciphertext
(enciphering key - specific process used to do this)

deciphering/decryption - restoring the plaintext from the ciphertext
(deciphering key - specific process used to do this)

cipher - method used to encipher/decipher

cryptanalysis - deciphering a ciphertext message without knowing the cipher
Modular Arithmetic

\( x \ (\text{mod } n) = r \) where \( r \) is the remainder when integer \( x \) is divided by \( n \) (\( n \) is a positive integer and \( 0 \leq r \leq n - 1 \)).

- \( 51 \ (\text{mod } 9) = 6 \) \((51 = 5 \cdot 9 + 6)\)
- \( 213 \ (\text{mod } 10) = 3 \) \((213 = 21 \cdot 10 + 3)\)
- \( 62 + 81 \ (\text{mod } 11) = 0 \) \((62 + 81 = 143 = 13 \cdot 11 + 0)\)
- \( 23^5 \ (\text{mod } 26) = 17 \) \((23^5 = 6436343 = 247551 \cdot 26 + 17)\)
- \( 13 \ (\text{mod } 26) = 13 \) \((13 = 0 \cdot 26 + 13)\)
Numerical Equivalents

<table>
<thead>
<tr>
<th>letter</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>NE:</td>
<td>00</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>letter</th>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>NE:</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>

LEAVING ON THE 1330 TRAIN TO PARIS.

11040021081306 1413 190704 1330 1917000813 1914 1500170818

11040 02108 13061 41319 07041 33019 17000 81319 14150 01708 18999
More Modular Arithmetic

Given a positive integer $n$ and an integer $x$ where $1 \leq x \leq n - 1$, the integer $x$ has an inverse $(\text{mod } n)$ if there exists an integer $y$, with $1 \leq y \leq n - 1$, such that $xy = 1 \pmod{n}$. In this case, $y = x^{-1} \pmod{n}$.

$3^{-1} \pmod{26} = 9$, $\quad 3 \cdot 9 \pmod{26} = 27 \pmod{26} = 1$

$4 \cdot 6 \pmod{26} = 24 \pmod{26} = 24$

$4 \cdot 7 \pmod{26} = 28 \pmod{26} = 02$

$4 \cdot 12 \pmod{26} = 48 \pmod{26} = 22$

$4 \cdot 13 \pmod{26} = 52 \pmod{26} = 00$

4 has no inverse $(\text{mod } 26)$. 
Problem

- Alice and Bob need a secure key exchange or need to share messages over a line watched by Eve. Must meet or communicate the details of the cipher (or message) over an insecure channel.

Solution

- James Ellis (1969) - worked for the British Government Communications Headquarters - not declassified (1997) until after his death. His idea was to add “noise” to create the ciphertext and then subtract it to get the plaintext.

- Whitefield Diffie & Martin Hellman (1976) - published “New Directions in Cryptography” after Diffie met with Ellis.
Symmetric Ciphers: Both Alice and Bob share or have equal knowledge of the secret key used to encrypt and decrypt messages.

Asymmetric or Public Key Ciphers: The key used to encrypt is distinct from the key used to decrypt and computing the deciphering method from the enciphering method is not feasible.

Public Key: Method used to encipher messages. This is created by Bob and anyone (even Eve) can know it.

Private Key: Method used to decipher the messages. This is also created by Bob and remains with him.
The Discrete Logarithm Problem

The field $\mathbb{F}_p^*$ is the collection of elements $\{1, 2, \ldots, p-2, p-1\}$ where if $x, y \in \mathbb{F}_p^*$, then $xy = xy \pmod{p}$.

Let $p$ be a prime number. Then there exists an element $g \in \mathbb{F}_p^*$ whose powers give every element of $\mathbb{F}_p^*$, i.e.

$$\mathbb{F}_p^* = \{1, g, g^2, \ldots, g^{p-2}, g^{p-1}\}$$

Elements with this property are called primitive roots of $\mathbb{F}_p^*$ or generators of $\mathbb{F}_p^*$. 
The Discrete Logarithm Problem

$\mathbb{F}_{11}^*$ has 2 as a primitive root.

\[
\begin{array}{ccccccc}
2^0 & = & 1 &  & 2^1 & = & 2 \\
2^2 & = & 4 &  & 2^3 & = & 8 \\
2^4 & = & 5 &  & 2^5 & = & 10 \\
2^6 & = & 9 &  & 2^7 & = & 7 \\
2^8 & = & 3 &  & 2^9 & = & 6 \\
\end{array}
\]

However, 2 is not a primitive root for $\mathbb{F}_{17}^*$.

\[
\begin{array}{ccccccc}
2^0 & = & 1 &  & 2^1 & = & 2 \\
2^2 & = & 4 &  & 2^3 & = & 8 \\
2^4 & = & 16 &  & 2^5 & = & 15 \\
2^6 & = & 13 &  & 2^7 & = & 9 \\
2^8 & = & 1 &  & 2^9 & = & 1 \\
\end{array}
\]
The Discrete Logarithm Problem

Let $g$ be a primitive root for $\mathbb{F}_p^*$ and let $h$ be an integer in $\mathbb{F}_p^*$. The **Discrete Logarithm Problem (DLP)** is the problem of finding an exponent $x$ such that

$$g^x = h \pmod{p}.$$ 

Given $\mathbb{F}_{941}^*$ with primitive root 627, only real way to solve the DLP $627^x = 551 \pmod{941}$ is to compute $627^1, 627^2, 627^3, \ldots$ until you get $627^{817} = 551 \pmod{941}$.

This is a **hard** problem.
The Discrete Logarithm Problem

Powers of $627^i \pmod{941}$ for $i = 1, 2, 3, \ldots$
Diffie-Hellman Key Exchange

Alice and Bob first agree on a large prime number $p$ and an integer $g$, where $1 \leq g \leq p - 1$, and make them public.

Alice picks a secret integer $a$ - Bob picks a secret integer $b$.

$$A = g^a \pmod{p} \quad \text{and} \quad B = g^b \pmod{p}$$

Alice computes this and Bob computes this.

Exchange Values

$$A' = B^a \pmod{p} \quad \text{and} \quad B' = A^b \pmod{p}$$

Alice computes this and Bob computes this.

$$A' = B^a = (g^b)^a = g^{ab} = (g^a)^b = A^b = B' \pmod{p}$$
**Diffie-Hellman Key Exchange**

Prime number $p = 7001$ Base $g = 101$

Alice picks $a = 300$ Bob picks $b = 2512$

\[
A = g^a \pmod{p} = 101^{300} \pmod{7001} = 1910
\]

\[
B = g^b \pmod{p} = 101^{2512} \pmod{7001} = 5533
\]

Exchange Values

\[
A' = B^a \pmod{p} = 5533^{300} \pmod{7001} = 5161
\]

\[
B' = A^b \pmod{p} = 1910^{2512} \pmod{7001} = 5161
\]
**Diffie-Hellman Key Exchange**

Eve knows $g, p, A = g^a$, and $B = g^b$. To find the private key, she must solve one of two DLPs.

Find $a$ by solving $g^a = A \pmod{p}$.

Find $b$ by solving $g^b = B \pmod{p}$.
RSA

- Create by Ron Rivest, Adi Shamir, and Len Adleman in 1978 at MIT.
- First public-key cipher.
- Still (as far as I know) widely used today.
RSA

1. Bob generates two distinct large prime numbers $p$ and $q$. He then computes $m = pq$ and $n = (p - 1)(q - 1)$.

$p = 103, q = 191$

$m = pq = 103 \cdot 191 = 19673, n = (p-1)(q-1) = 102 \cdot 190 = 19380$

- $p$ and $q$ should each be of binary length 1024 (309 digits) or larger.
- $p$ and $q$ should approximately be of the same size.
- Here all of the calculations take place in

$\mathbb{F}_{pq}^* = \{x | 1 \leq x \leq pq - 1 \text{ and } x \text{ and } pq \text{ are relatively prime}\}$. 
RSA

2 Bob selects a number $e$ that is relatively prime to $n$.

Pick $e = 23 \cdot 29 = 667$ \hspace{1cm} n = 19380 = 2^2 \cdot 3 \cdot 5 \cdot 17 \cdot 19$

3 Bob finds $d$ such that $ed = 1 \pmod{n}$ (use Euclidean Algorithm).

\hspace{1cm} d = 523

4 Bob makes $e = 667$ and $m = 19763$ public (public key). Security based on the ability to factor $m$. 
RSA

5 Alice arranges message as a series of numbers $x$ such that $0 \leq x \leq m - 1$ or $0 \leq x \leq 19672$.

6 For each number $x$, Alice computes $y = x^e \pmod{m}$ or $y = x^{667} \pmod{19673}$.
RSA

7 Alice sends the ciphertext to Bob and he deciphers it using his private key $d$ and $n$. Bob computes $x = y^d \pmod{m}$ or $x = y^{523} \pmod{19673}$.

Comments:

- $x \rightarrow x^e \pmod{m} \rightarrow (x^e)^d \pmod{m} = x^{ed} \pmod{m} = x$
- As factoring methods improve, need to find larger primes (safe here as there are an infinite number of primes).
- Or, we could make the algebra harder.
A Little Group Theory

Generalize $\mathbb{F}_p^*$ with operation $x \cdot y = xy \ (\text{mod} \ p)$ to a non-abelian (non-commutative) group. A group is a collection of objects with a binary operation $\star$ such that

- $(x \star y) \star z = x \star (y \star z)$,
- there exists identity $e$ where $x \star e = e \star x = x$, and
- for each $x$ the element $x^{-1}$ exists such that $x \star x^{-1} = x^{-1} \star x = e$. 
Elliptic Curve Cryptography

An **elliptic curve** \( E \) is the set of solutions to the equation of the form

\[
Y^2 = X^3 + AX + B.
\]

together with an extra point \( \mathcal{O} \), where the constants \( A \) and \( B \) satisfy \( A^3 + 27B^2 \neq 0 \).
You can define an operation (way to add points) on the points of an elliptic curve.
Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on the elliptic curve $y^2 = x^3 + Ax + B$.

a) If $P_1 = O$, then $P_1 + P_2 = P_2$.
b) If $P_2 = O$, then $P_1 + P_2 = P_1$.
c) If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = O$.
d) Otherwise, define $\lambda$ by

$$
\lambda = \begin{cases} 
\frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\
\frac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2
\end{cases}
$$

and let

$$
x_3 = \lambda^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \lambda(x_1 - x_3) - y_1.
$$

Then $P_1 + P_2 = (x_3, y_3)$. 
Elliptic Curve Cryptography
Elliptic Curve Cryptography

\[ L \text{ is tangent to } E \text{ at } P \]

\[ 2P = P \oplus P = R' \]
Elliptic Curve Cryptography

- \( P = (a, b) \)
- \( P' = (a, -b) \)
Elliptic Curve over Finite Fields

\[ \mathbb{F}_p = \{0, 1, \ldots, p - 1\} \]

\[ E : Y^2 = X^3 + AX + B \text{ with } A, B \in \mathbb{F}_p \]

\[ E(\mathbb{F}_p) = \{(x, y) \mid x, y \in \mathbb{F}_p \text{ satisfying } y^2 = x^3 + Ax + B\} \cup \{O\} \]
Elliptic Curve over Finite Fields

\[ \mathbb{F}_{13} = \{0, 1, \ldots, 12\} \]

\[ E : Y^2 = X^3 + 3X + 8 \]

\[ E(\mathbb{F}_{13}) = \{ \mathcal{O}, (1, 5), (1, 8), (2, 3), (2, 10), (9, 6), (9, 7), (12, 2), (12, 11) \} \]

\[ (1, 5) \oplus (9, 6) = (2, 3) \quad (12, 2) \oplus (2, 10) = (9, 6) \]
Elliptic Curve Discrete Log Problem (ECDLP)

Let $P$ be a point on $E(\mathbb{F}_p)$. Let $n$ be a positive integer and compute $Q = nP = P \oplus P \oplus \cdots \oplus P$. Publish $P$ and $Q$.

The ECDLP is to find $n$ such that

$$Q = nP.$$ 

The ECDLP is “harder” than the DLP.

Fastest DLP Solution Method - order of $\log p$.
Fastest ECDLP Solution Method - order of $\sqrt{p}$.
Elliptic Curve Diffie-Hellman Key Exchange

Alice and Bob first agree on a large prime number $p$, and elliptic curve $E$, and a point $P \in E(\mathbb{F}_p)$.

Alice picks a secret integer $a$ - Bob picks a secret integer $b$.

\[
Q_1 = aP = (P + \cdots + P)
\]

Alice computes this

\[
Q_2 = bP = (P + \cdots + P)
\]

Bob computes this

Exchange Values

\[
R' = aQ_2 = (Q_2 + \cdots + Q_2)
\]

Alice computes this

\[
S' = bQ_1 = (Q_1 + \cdots Q_1)
\]

Bob computes this

\[
R' = aQ_2 = a(bP) = abP = b(aP) = b(Q_1) = S'
\]
Elliptic ElGamal Public Key Cryptosystem

1. Alice and Bob agree on $p$, the elliptic curve $E$, and point $P \in E(\mathbb{F}_p)$.
2. Bob chooses $n_B$ and publishes $Q_B = n_B P$ as public key.
3. Alice’s plaintext is a point $M \in E(\mathbb{F}_p)$.
4. Alice chooses an integer $k$ and computes
   
   $$C_1 = kP \quad \text{and} \quad C_2 = M + kQ_B$$

5. Alice send the two points $C_1$ and $C_2$ to Bob.
6. Bob computes the following to obtain the plaintext $M$.

   $$C_2 - n_B C_1 = (M + kQ_B) - n_B (kP) = M + k(n_B P) - n_B (kP) = M$$
Elliptic ElGamal Public Key Cryptosystem

1. Alice and Bob agree on $p = 3851$, the elliptic curve $E : y^2 = x^3 + 324x + 1287$, and point $P = (920, 303) \in E(\mathbb{F}_{3851})$.

2. Bob chooses $n_B = 2489$ and publishes $Q_B = n_B P = 2489(920, 303) = (593, 719)$ as public key.

3. Alice’s plaintext is a point $M = (3681, 612) \in E(\mathbb{F}_p)$.

4. Alice chooses an integer $k = 3021$ and computes

   $$C_1 = kP = 3021(920, 303) = (343, 3454)$$

   and

   $$C_2 = M + kQ_B = (3681, 612) + 3021(593, 719)$$
   $$= (3681, 612) + (252, 3610) = (3506, 686)$$
Elliptic ElGamal Public Key Cryptosystem

5. Alice sends the two points $C_1 = (343, 3454)$ and $C_2 = (3506, 686)$ to Bob.

6. Bob computes the following to obtain the plaintext $M$.

\[
M = C_2 - n_B C_1 = (3506, 686) - 2489(343, 3454) \\
= (3506, 686) - (252, 3610) \\
= (3681, 612)
\]