Number Theory, Polynomials, and the Advanced Encryption Standard

Joshua Holden
Rose-Hulman Institute of Technology
http://www.rose-hulman.edu/~holden

Question What does cryptography have to do with number theory?

Answer Everything.

Shift (Caesar) ciphers, atbash cipher modular arithmetic

Affine ciphers gcds, Euclidean algorithm, modular inverses

Pohlig-Hellman exponentiation cipher Fermat's Little Theorem, primality testing

RSA Euler's phi function, Euler's Theorem, factorization

Data Encryption Standard (DES) (not much)

Advanced Encryption Standard (AES) modular arithmetic with *polynomials*

Two principles of modern cryptography

diffusion Each plaintext digit affects the value of many ciphertext digits and vice versa.

confusion The relationship between the structure of the ciphertext and the structure of the key is as complicated as possible.

AES

- Multiple rounds
- Four stages in each round:
  - Substitute (confusion) "S-box"
  - Shift (diffusion)
  - Mix (diffusion)
  - Add key

Types of S-boxes

- Random
- Random with testing
- Human-made
- Math-made

DES uses "human-made" S-boxes

AES uses "math-made" S-boxes — the math is polynomial modular arithmetic

S-AES (Simplified Advanced Encryption Standard) is a simplified version of AES invented by Mohammad Musa, Edward Schaefer, and Stephen Wedig for teaching purposes.

Parameter	AES	S-AES
Key size	16 bytes/128 bits	4 "nibbles"/16 bits
Plaintext block size	16 bytes/128 bits	4 "nibbles"/16 bits
Number of rounds	10	2

Question: How do you multiply two 4-bit nibbles and get another 4-bit nibble?

One way is to translate them into polynomials:

$$1010 \rightarrow 1x^3 + 0x^2 + 1x + 0$$

$$= x^3 + x$$

$$0101 \rightarrow 0x^3 + 1x^2 + 0x + 1$$

$$= x^2 + 1$$

and then multiply the polynomials:

$$x^5 + 2x^3 + x$$

Oops. We wanted bits. We could reduce the coefficients modulo 2:

$$x^5 + x$$

But we still have 6 bits and we wanted 4. The solution is to reduce modulo a degree 4 irreducible (prime) polynomial.

We could pick any polynomial we wanted as long as we are consistent. The S-AES designers picked $x^4 + x + 1$.

Reducing modulo a polynomial is just like reducing modulo a number — divide and take the remainder.

(For algebra geeks, we are working in the field

$$\mathrm{GF}(2^4) = \mathbb{Z}_2[x]/(x^4 + x + 1). \quad)$$

$$
\begin{array}{r}
\multicolumn{1}{r}{x} \\
\cline{2-2}
x^4 + x + 1 \big) \; x^5 \qquad + x \\
\multicolumn{1}{r}{- x^5 - x^2 - x} \\
\cline{2-2}
\multicolumn{1}{r}{- x^2}
\end{array}
$$

The remainder is $-x^2$, which is the same as x^2 modulo 2. Clearly when we are done the degree is less than 4, so we can convert it back to a nibble:

$$x^2 \rightarrow 0100$$

Or in the AES notation:

$$1010 \bullet 0101 = 0100$$

This multiplication is used in the Mix step.

The Substitute step, or S-box, uses polynomial modular arithmetic as above combined with polynomial modular inverses.

We find these using the Euclidean algorithm, just as we do in integer modular arithmetic.

$$1100 \rightarrow 1x^3 + 1x^2 + 0x + 0$$

$$= x^3 + x^2$$

We start by finding the greatest common divisor of $x^3 + x^2$ and $x^4 + x + 1$.

$$\begin{aligned}
x^4 + x + 1 &= \left(x^3 + x^2\right) \cdot \left(x - 1\right) + \left(x^2 + x + 1\right) \\
x^3 + x^2 &= \left(x^2 + x + 1\right) \cdot x + -x \\
x^2 + x + 1 &= -x \cdot \left(-x - 1\right) + 1 \\
-x &= 1 \cdot -x + 0
\end{aligned}$$

Reducing modulo 2 whenever convenient, we can rewrite that as:

$$\begin{aligned}
x^2 + x + 1 &= x^4 + x + 1 - (x^3 + x^2) \cdot (x + 1) \\
x &= x^3 + x^2 - x \cdot (x^2 + x + 1) \\
1 &= x^2 + x + 1 - (x + 1) \cdot (x)
\end{aligned}$$

and substituting:

$$\begin{array}{rcrcl} x^2+x+1 & = & x^4+x+1 & + & (x^3+x^2)\cdot(x+1) \\ x & = & (x^2+x+1)\cdot(x^3+x^2) & + & x\cdot(x^4+x+1) \\ 1 & = & (x^3+x)\cdot(x^3+x^2) & + & (x^2+x+1)\cdot(x^4+x+1) \end{array}$$

The last line, reducing modulo x^4+x+1, shows that the inverse of x^3+x^2 modulo x^4+x+1 is x^3+x.

Or in the AES notation:

$$(1100)^{-1} = 1010$$

There's a lot of other number theory and algebra in AES, also:

- lots of arithmetic modulo 2
- matrix arithmetic in both $\mathbb{Z}_2$ and GF(2^8).
- polynomials with coefficients in GF(2^8).
- polynomial arithmetic in GF(2^8)$[X]/(X^4 + 1)$.

Where could you use this?

- Cryptography courses
- Number theory courses
- Algebra courses
- ???

Enjoy!