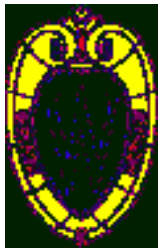

CS/ECE/Math 435
Introduction to Cryptography

Professor Chris DeMarco
Department of Electrical & Computer Engineering
University of Wisconsin-Madison

Spring Semester 2021

Goal: Describe key ideas of the Advanced Encryption Standard (AES), analogous to our treatment of DES.

Necessary Background: A particular construction of Finite Fields (synonomous with "Galois Field"), based on polynomials on $\mathbb{Z}_2$.

Q: WHY (do we need these finite fields built of polynomials on $\mathbb{Z}_2$)?

Ans: Remember that critical to improved security of encryption is incorporation of a nonlinear function, that must be invertible.

In DES, this was accomplished with low-dimensional Boolean functions set by look-up tables, combined with the Feistel construction to make them invertible.

In AES, we will use the inverse function itself (with the inverse operation on $GF(2^8)$

Desirable properties for our new sets, that are going to "replace" $\mathbb{Z}_N$ in our analysis of AES:

i) We'd like them to have number of elements $= 2^n$ (specifically 2^8 for AES), so we have easy "book-keeping" of elements via n-bit binary word.

ii) Because we want to be able to use the inverse operation, every non-zero element of the set must be invertible.

Observe that the combination of (i) & (ii) rules out use of $\mathbb{Z}_N$ with $N = 2^n$ (e.g., $N = 2^8$), because not every non-zero element will be invertible.

Remember what we need for our algebraic approach to encryption functions

- a zero element
- a unity element
- well defined addition
- well defined multiplication

And now, based on (ii), we want a multiplicative inverse for every non-zero element.

These are properties that define a Galois Field. Common notation "GF(q)" denotes Galois Field having q elements (we'll want $GF(2^8)$ for AES)

Q1: So, if integers with mod N arithmetic don't work, what type of elements can we use?

A1: Elements of our set will be polynomials with coefficients in $\mathbb{Z}_2$ (i.e. coefficients $\{0, 1\}$).

Q2: And by analogy to case of $\mathbb{Z}_N$ with arithmetic mod N, what type of $+$, $\cdot$ operations can we use?

A2: (here where all the work lies) polynomial algebra, modulo an irreducible polynomial f.

So, A2 really involves a particular approach to building a $GF(q = 2^n)$. Think of this as a generalization of our Z_N sets used earlier in 435.

- Starting point: select an <u>irreducible</u> polynomial on Z_2 of degree n, denote this f. To be irreducible, f is <u>not</u> factorable as product of two or more lower degree polynomials.

- Elements of the set are all polynomials on $\mathbb{Z}_2$ of degree $< n$.

Example: Suppose $n = 3$.

A choice of an irreducible $f = x^3 + x + 1$.

Polynomials in our set:	Binary word "shorthand"
0) $0 \cdot x^2 + 0 \cdot x^1 + 0$	0 0 0
1) $0 \cdot x^2 + 0 \cdot x^1 + 1$	0 0 1
2) $0 \cdot x^2 + 1 \cdot x^1 + 0$	0 1 0
3) $0 \cdot x^2 + 1 \cdot x^1 + 1$	0 1 1
4) $1 \cdot x^2 + 0 \cdot x^1 + 0$	1 0 0
5) ⋮ ⋮ ⋮	1 0 1
6) ⋮ ⋮ ⋮	1 1 0
7) ⋮ ⋮ ⋮	1 1 1

- Addition operation: easy - just add like-order coefficients mod 2

- Multiply operation: somewhat harder - we're computing "u × v mod f."
  i) Perform "ordinary" polynomial multiply, albeit in $\mathbb{Z}_2$. Denote this intermediate result "p."
  ii) Observe that resulting polynomial can have degree $\geq n$, so it is not (initially) a member of our set. FIX...

Perform long polynomial division $p \div f$ or $f\overline{)p}$. This will yield a quotient polynomial, q, and a remainder polynomial, r.

Define $[u \times v \mod f] = r$

Note that this is analogous to our work with $\mathbb{Z}_N$, but now with polynomial long division.

Aside: Sets Z_N had every nonzero element invertible when N selected to be a prime number.

Sets of polynomials have every nonzero element invertible when f selected to be an irreducible polynomial.

For given degree n, selection of irreducible polynomial is not unique, but seemingly different f's yield equivalent $GF(2^n)$ systems.

Using our $GF(2^3)$ example with $f = X^3 + X + 1$, how to compute inverse elements?

(again, this is the whole point for AES - we want to use the inverse operation as our critical nonlinear function in the encryption process).

Recall that early in 435 (see Bach notes section 3), we saw that Euclid's algorithm could be used to compute inverse elements in $\mathbb{Z}_N$. Exact same algorithm (see table form, Bach notes p. 3-4) works to compute inverses elements in $GF(2^n)$, but with added complication of polynomial long division replacing integer division.

To compute a^{-1} build a four column table

row #	Column q	Column d	Column x	Column y
Initialize 1	empty	$d_1 = f$	$x_1 = 1$	$y_1 = 0$
2	empty	$d_2 = a$	$x_2 = 0$	$y_2 = 1$
3	Compute $d_1 \div d_2$ q_3 = quotient	$d_1 \div d_2$ d_3 = remainder	$x_3 = x_1 - q_3 \cdot x_2$	$y_3 = y_1 - q_3 \cdot y_2$
4	Compute $d_2 \div d_3$ q_4 = quotient	$d_2 \div d_3$ d_4 = remainder	$x_4 = x_2 - q_4 \cdot x_3$	$y_4 = y_2 - q_4 \cdot y_3$
	$d_3 \div d_4$ $\vdots$	$d_3 \div d_4$ $\vdots$		

terminate when $d_k = 1$

Important property of this tabular computation: in each row, by construction $d_k = f \cdot x_k + a \cdot y_k$.

So at termination, when $d_k = 1$, one has:

$$1 = a \cdot y_k + f \cdot x_k$$

with degree $(y_k) < n \Rightarrow$

y_k is an element of our set of all polynomials on $\mathbb{Z}_2$ with degree $< n$, and $(a \cdot y_k) \bmod f = 1$

$\Rightarrow Y_k$ must $= a^{-1}$!

Example: Again, for $GF(2^3)$ constructed with $f = x^3 + x + 1$, compute inverse $(x^2 + x)$.

Euclid Table to compute $(x^2+x)^{-1}$, mod (x^3+x+1) (17)

	q	d	x	y
1)	–	x^3+x+1	1	0
2)	–	x^2+x	0	1
3)	x	x^2+x+1	1	x
	1	(1) terminate	1	$x+1$

Intermediate calculations:

@ row 3: $(x^2+x+1) \div (x^2+x) \rightarrow \begin{cases} \text{quotient} & x \\ \text{remainder} & x^2+x+1 \end{cases}$

@ row 4 $(x^2+x) \div (x^2+x+1) \rightarrow \begin{cases} \text{quotient} & 1 \\ \text{remainder} & 1 \end{cases}$

And by construction, we should have:

$$1 \overset{?}{=} \Big[\underbrace{(x^2+x)}_{\text{our original "a" polynomial}} \quad \underbrace{(x+1)}_{y_4}\Big] + \Big[\underbrace{1}_{x_4} \cdot (x^3+x+1)\Big]$$

$$= \Big[\cancel{x^3} + \cancel{x^2} + \cancel{x^2} + x\Big] + \Big[\cancel{x^3} + \cancel{x} + 1\Big]$$

$$\overset{\checkmark}{=} 1 \quad \Rightarrow (x^2+x)^{-1} = x+1$$

shorthand $\quad [1 \;\; 1 \;\; 0]^{-1} = [0 \;\; 1 \;\; 1]$