- Recall that, in contrast to DES, the operations of AES have very simple (though somewhat advanced) mathematical descriptions.

  No mysteriously constructed S-boxes and P-boxes as in DES.

ByteSub (continued)

Each of the 16 bytes gets substituted as follows.

Note. The mathematical description below can be implemented in a **lookup table**: you can find this table in Table 5.1 of our book or, for instance, on wikipedia: https://en.wikipedia.org/wiki/Rijndael_S-box

- Interpret the input byte $(b_7b_6...b_0)_2$ as the element $b_7x^7+...+b_1x+b_0$ of $\mathrm{GF}(2^8)$.
- Compute $s^{-1}=c_0+c_1x+...+c_7x^7$ (with 0^{-1} interpreted as 0).

  Important comment. This inversion is what makes AES highly nonlinear.

  If the ByteSub substitution was linear, then all of AES would be linear (because all other layers are linear; assuming we adjust the key schedule accordingly).

- Then the output bits $(d_7d_6...d_1d_0)_2$ are

$$\begin{bmatrix} d_0 \\ d_1 \\ \vdots \\ d_7 \end{bmatrix} = \begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

Comment. The particular choice of matrix and vector has the effect that no ByteSub output equals the ByteSub input (or its complement).

Example 139. Invert x^3+1 in $\mathrm{GF}(2^8)$, constructed as in AES. [Example 136, again]

Solution. We use the extended Euclidean algorithm, and always reduce modulo 2:

$$\begin{aligned} \boxed{x^8+x^4+x^3+x+1} &\equiv (x^5+x^2+x+1)\cdot\boxed{x^3+1}+x^2 \\ \boxed{x^3+1} &\equiv x\cdot\boxed{x^2}+1 \end{aligned}$$

Backtracking through this, we find that Bézout's identity takes the form

$$\begin{aligned} 1 \equiv 1\cdot\boxed{x^3+1}-x\cdot\boxed{x^2} &\equiv 1\cdot\boxed{x^3+1}-x\cdot\left(\boxed{x^8+x^4+x^3+x+1}-(x^5+x^2+x+1)\cdot\boxed{x^3+1}\right) \\ &\equiv (x^6+x^3+x^2+x+1)\cdot\boxed{x^3+1}+x\cdot\boxed{x^8+x^4+x^3+x+1}. \end{aligned}$$

Hence, $(x^3+1)^{-1}=x^6+x^3+x^2+x+1$ in $\mathrm{GF}(2^8)$.

Example 140. (homework)

(a) What happens to the byte $(0000\ 0101)_2$ during ByteSub?

(b) What happens to the byte $(0000\ 1001)_2$ during ByteSub?

Solution.

(a) $(0000\ 0101)_2$ represents the polynomial x^2+1.
By the previous example, its inverse is $(x^2+1)^{-1} = x^6+x^4+x$ in $\mathrm{GF}(2^8)$, which is $\boldsymbol{c} = (0101\ 0010)_2$.

$$\begin{bmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{bmatrix} \underbrace{\begin{bmatrix} 0\\1\\0\\0\\1\\0\\1\\0 \end{bmatrix}}_{\boldsymbol{c}} + \begin{bmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{bmatrix} = \begin{bmatrix} 0\\1\\1\\1\\1\\1\\0\\0 \end{bmatrix} + \begin{bmatrix} 1\\0\\0\\0\\1\\1\\1\\1 \end{bmatrix} + \begin{bmatrix} 1\\1\\1\\0\\0\\0\\1\\1 \end{bmatrix} + \begin{bmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{bmatrix} = \begin{bmatrix} 1\\1\\0\\1\\0\\1\\1\\0 \end{bmatrix}$$

[This is just the usual matrix-vector product modulo 2. The highlighted columns are the ones which get added up during this matrix-vector product.]

Hence, the output of ByteSub is the byte $(0110\ 1011)_2$.

Check with lookup tables. Indeed, our computation matches $107 = (0110\ 1011)_2$ in the lookup table in our book (row 0, column $(0101)_2 = 5$) or $(6\mathrm{B})_{16} = (0110\ 1011)_2$ on wikipedia (row $(0000)_2 = (0)_{16}$, column $(0101)_2 = (5)_{16}$).

(b) $(0000\ 1001)_2$ represents the polynomial x^3+1.
By the previous example, $(x^3+1)^{-1} = x^6+x^3+x^2+x+1$ in $\mathrm{GF}(2^8)$, which is $\boldsymbol{c} = (0100\ 1111)_2$.

$$\begin{bmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{bmatrix} \underbrace{\begin{bmatrix} 1\\1\\1\\1\\0\\0\\1\\0 \end{bmatrix}}_{\boldsymbol{c}} + \begin{bmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{bmatrix} = \begin{bmatrix} 1\\1\\1\\1\\1\\0\\0\\0 \end{bmatrix} + \begin{bmatrix} 0\\1\\1\\1\\1\\1\\0\\0 \end{bmatrix} + \begin{bmatrix} 0\\0\\1\\1\\1\\1\\1\\0 \end{bmatrix} + \begin{bmatrix} 0\\0\\0\\1\\1\\1\\1\\1 \end{bmatrix} + \begin{bmatrix} 1\\1\\1\\0\\0\\0\\1\\1 \end{bmatrix} + \begin{bmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{bmatrix} = \begin{bmatrix} 1\\0\\0\\0\\0\\0\\0\\0 \end{bmatrix}$$

Hence, the output of ByteSub is the byte $(0000\ 0001)_2$.

Check with lookup tables. Indeed, our computation matches the value 1 in the lookup table in our book (row 0, column $(1001)_2 = 9$) or $(01)_{16}$ on wikipedia (row $(0000)_2 = (0)_{16}$, column $(1001)_2 = (9)_{16}$).

Review: multiplicative order and primitive roots

Definition 141. The **multiplicative order** of an invertible residue a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Important note. By Euler's theorem, the multiplicative order can be at most $\phi(n)$.

Example 142. What is the multiplicative order of $2 \pmod 7$?

Solution. $2^1 = 2$, $2^2 = 4$, $2^3 \equiv 1 \pmod 7$. Hence, the multiplicative order of $2 \pmod 7$ is 3.

Definition 143. If the multiplicative order of an residue a modulo n equals $\phi(n)$ [in other words, the order is as large as possible], then a is said to be **primitive root** modulo n.

A primitive root is also referred to as a **multiplicative generator** (because the products of a and itself, that is, $1, a, a^2, a^3, \ldots$, produce all invertible residues).

Example 144. What is the multiplicative order of $3 \pmod 7$?

Solution. $3^1 = 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1$. Hence, the multiplicative order of $3 \pmod 7$ is 6. This means that 3 is a primitive root modulo 7. Note how every (invertible) residue shows up as a power of 3.

Review. $x \pmod n$ is a primitive root.

$\iff$ The (multiplicative) order of $x \pmod n$ is $\phi(n)$. (That is, the order is as large as possible.)

$\iff$ $x, x^2, \ldots, x^{\phi(n)}$ is a list of all invertible residues modulo n.

Lemma 145. If $a^r \equiv 1 \pmod n$ and $a^s \equiv 1 \pmod n$, then $a^{\gcd(r,s)} \equiv 1 \pmod n$.

Proof. By Bezout's identity, there are integers x, y such that $xr + ys = \gcd(r,s)$.
Hence, $a^{\gcd(r,s)} = a^{xr+ys} = a^{xr}a^{ys} = (a^r)^x (a^s)^y \equiv 1 \pmod n$. □

Corollary 146. The multiplicative order of a modulo n divides $\phi(n)$.

Proof. Let k be the multiplicative order, so that $a^k \equiv 1 \pmod n$. By Euler's theorem $a^{\phi(n)} \equiv 1 \pmod n$. The previous lemma shows that $a^{\gcd(k,\phi(n))} \equiv 1 \pmod n$. But since the multiplicative order is the smallest exponent, it must be the case that $\gcd(k, \phi(n)) = k$. Equivalently, k divides $\phi(n)$. □

Comment. By the same argument, if $a^m \equiv 1 \pmod n$, then the order of $a \pmod n$ divides m.

Example 147. Compute the multiplicative order of 2 modulo $7, 11, 9, 15$. In each case, is 2 a primitive root?

Solution.

- $2 \pmod 7$: $2^2 \equiv 4, 2^3 \equiv 1$. Hence, the order of 2 modulo 7 is 3.
  Since the order is less than $\phi(7) = 6$, 2 is not a primitive root modulo 7.
- $2 \pmod{11}$: Since $\phi(11) = 10$, the only possible orders are $2, 5, 10$. Hence, checking that $2^2 \not\equiv 1$ and $2^5 \not\equiv 1$ is enough to conclude that the order must be 10.
  Since the order is equal to $\phi(11) = 10$, 2 is a primitive root modulo 11.
  Brute force approach (too much unnecessary work). Just for comparison, $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 5, 2^5 \equiv 2 \cdot 5 = 10, 2^6 \equiv 2 \cdot 10 \equiv 9, 2^7 \equiv 2 \cdot 9 \equiv 7, 2^8 \equiv 2 \cdot 7 \equiv 3, 2^9 \equiv 2 \cdot 3 = 6, 2^{10} \equiv 2 \cdot 6 \equiv 1$. Thus, the order of 2 mod 11 is 10.
- $2 \pmod 9$: Since $\phi(9) = 6$, the only possible orders are $2, 3, 6$. Hence, checking that $2^2 \not\equiv 1$ and $2^3 \not\equiv 1$ is enough to conclude that the order must be 6. (Indeed, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1$.)
  Since the order is equal to $\phi(9) = 6$, 2 is a primitive root modulo 9.
- The order of $2 \pmod{15}$ is 4 (a divisor of $\phi(15) = 8$).
  2 is not a primitive root modulo 15. In fact, there is no primitive root modulo 15.

Comment. It is an open conjecture to show that 2 is a primitive root modulo infinitely many primes. (This is a special case of Artin's conjecture which predicts much more.)

Advanced comment. There exists a primitive root modulo n if and only if n is of one of $1, 2, 4, p^k, 2p^k$ for some odd prime p.

Example 148. Show that $x^4 \equiv 1 \pmod{15}$ for all invertible residues $x \pmod{15}$. In particular, there are no primitive roots modulo 15.

Solution. By the Chinese Remainder Theorem:

$x^4 \equiv 1 \pmod{15}$
$\iff$ $x^4 \equiv 1 \pmod 3$ and $x^4 \equiv 1 \pmod 5$

The congruences modulo 3 and 5 follow immediately from Fermat's little theorem.

Comment. The same argument shows that there are no primitive roots modulo pq, where p and q are distinct odd primes (because each element has order dividing $\phi(pq)/2$).

Armin Straub
straub@southalabama.edu

Lemma 149. Suppose $x \pmod n$ has (multiplicative) order k.

(a) $x^a \equiv 1 \pmod n$ if and only if $k|a$.

(b) x^a has order $\frac{k}{\gcd(k,a)}$.

Proof.

(a) "$\Longrightarrow$": By Lemma 145, $x^k \equiv 1$ and $x^a \equiv 1$ imply $x^{\gcd(k,a)} \equiv 1 \pmod n$. Since k is the smallest exponent, we have $k = \gcd(k,a)$ or, equivalently, $k|a$.
"$\Longleftarrow$": Obviously, if $k|a$ so that $a = kb$, then $x^a = (x^k)^b \equiv 1 \pmod n$.

(b) By the first part, $(x^a)^m \equiv 1 \pmod n$ if and only if $k|am$. The smallest such m is $m = \frac{k}{\gcd(k,a)}$. □

Example 150. Determine the orders of each (invertible) residue modulo 7. In particular, determine all primitive roots modulo 7.

Solution. First, observe that, since $\phi(7) = 6$, the orders can only be $1, 2, 3, 6$. Indeed:

residues	1	2	3	4	5	6
order	1	3	6	3	6	2

The primitive roots are 3 and 5.

Example 151. Redo Example 150, starting with the knowledge that 3 is a primitive root.

Solution.

residues	1	2	3	4	5	6
3^a	3^0	3^2	3^1	3^4	3^5	3^3
order$=\frac{6}{\gcd(a,6)}$	$\frac{6}{6}$	$\frac{6}{2}$	$\frac{6}{1}$	$\frac{6}{2}$	$\frac{6}{1}$	$\frac{6}{3}$

RSA and public key cryptography

- So far, our symmetric ciphers required a single **private key** k, a secret shared between the communicating parties.

  That leaves the difficult task of how to establish such private keys over a medium like the internet.

- In **public key cryptosystems**, there are two keys k_e, k_d, one for encryption and one for decryption. Bob keeps k_d secret (from anyone else!) and shares k_e with the world. Alice (or anyone else) can then send an encrypted message to Bob using k_e. However, Bob is the only who can decrypt it using k_d.

  It is crucial that the key k_d cannot be (easily) constructed from k_e.

RSA is one the first public key cryptosystems.

- It was described by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. (Note the initials!)
- However, a similar system had already been developed in 1973 by Clifford Cocks for the UK intelligence agency GCHQ (classified until 1997). Even earlier, in 1970, his colleague James Ellis was likely the first to discover public key cryptography.

Example 152. Let us emphasize that it should be surprising that something like public key cryptography is even possible.

Imagine Alice, Bob and Eve sitting at a table. Everything that is being said is heard by all three of them. The three have never met before and share no secrets. Should it be possible in these circumstances that Alice and Bob can share information without Eve also learning about it?

Public key cryptography makes exactly that possible!

Comments on primitive roots

Example 153. Determine all primitive roots modulo 11.

Solution. Since $\phi(11)=10$, the possible orders of residues modulo 11 are $1,2,5,10$. Residues with order 10 are primitive roots. Our strategy is to find one primitive root and to use that to compute all primitive roots.
There is no good way of finding the first primitive root. We will just try the residues $2,3,5,\ldots$ (why not 4?!)
We compute the order of $2 \pmod{11}$:
Since $2^2=4\not\equiv 1$, $2^5\equiv -1\not\equiv 1 \pmod{11}$, we find that 2 has order 10. Hence, 2 is a primitive root.
All other invertible residues are of the form 2^x. Recall that the order of $2^x \pmod{11}$ is $\frac{10}{\gcd(10,x)}$.
Hence, 2^x is a primitive root if and only if $\gcd(10,x)=1$, which yields $x=1,3,7,9$.
In conclusion, the primitive roots modulo 11 are $2^1=2, 2^3=8, 2^7\equiv 7, 2^9\equiv 6$.

Example 154. (extra) Determine all primitive roots modulo 22.

Solution. We proceed as in the previous example:

- Since $\phi(22)=10$, the possible orders of residues modulo 22 are $1,2,5,10$.
- We find one primitive root by trying residues $3,5,\ldots$ (2 is out because it is not invertible modulo 22)
  Since $3^5\equiv 1 \pmod{22}$, 3 is not a primitive root modulo 22.
  Since $5^5\equiv 1 \pmod{22}$, 5 is not a primitive root modulo 22.
  Since $7^2\not\equiv 1$, $7^5\equiv -1\not\equiv 1 \pmod{22}$, 7 is a primitive root modulo 22.
- $7^x \pmod{22}$ has order $\frac{10}{\gcd(10,x)}$. We have $\gcd(10,x)=1$ for $x=1,3,7,9$.
- Hence, the primitive roots modulo 22 are $7^1=7, 7^3\equiv 13, 7^7\equiv 17, 7^9\equiv 19$.

Proceeding as in the previous example, we obtain the following result.

Theorem 155. (number of primitive roots) Suppose there is a primitive root modulo n. Then there are $\phi(\phi(n))$ primitive roots modulo n.

Proof. Let x be a primitive root. It has order $\phi(n)$. All other invertible residues are of the form x^a.
Recall that x^a has order $\frac{\phi(n)}{\gcd(\phi(n),a)}$. This is $\phi(n)$ if and only if $\gcd(\phi(n),a)=1$. There are $\phi(\phi(n))$ values a among $1,2,\ldots,\phi(n)$, which are coprime to $\phi(n)$.
In conclusion, there are $\phi(\phi(n))$ primitive roots modulo n. □

Comment. Recall that, for instance, there is no primitive root modulo 15. That's why we needed the assumption that there should be a primitive root modulo n (which is the case if and only if n is of the form $1,2,4,p^k,2p^k$ for some odd prime p).

In particular, since there are always primitive roots modulo primes, we have the following important case:

There are $\phi(\phi(p))=\phi(p-1)$ primitive roots modulo a prime p.

Example 156. (bonus challenge) For which prime $p<10^6$ is the proportion of primitive roots among invertible residues the smallest?

Send in a solution by next week for a bonus point!

Armin Straub
straub@southalabama.edu

Back to RSA

(RSA encryption)

- Bob chooses large random primes p, q.
- Bob chooses e, and then computes d such that $de \equiv 1 \pmod{(p-1)(q-1)}$.
- Bob makes $N = pq$ and e public. His (secret) private key is d.
- Alice encrypts $c = m^e \pmod{N}$.
- Bob decrypts $m = c^d \pmod{N}$.

Does decryption always work? What Bob computes is $c^d \equiv (m^e)^d = m^{de} \pmod{N}$. It follows from Euler's theorem and $de \equiv 1 \pmod{\phi(N)}$ that $m^{de} \equiv m \pmod{\phi(N)}$ for all invertible residues m. That this actually works for all residues can be seen from the Chinese Remainder Theorem (see Theorem 157 below).

Is that really secure? Well, if implemented correctly (we will discuss potential issues), RSA has a good track record of being secure. Next class, we will actually prove that finding the secret key d is as difficult as factoring N (which is believed, but has not been proven, to be hard). On the other hand, it remains an important open problem whether knowing d is actually necessary to decrypt a given message.

Comment. The $(p-1)(q-1)$ in the generation of d can be replaced with $\operatorname{lcm}(p-1, q-1)$. This will be illustrated in Example 161.

Theorem 157. Let $N = pq$ and d, e be as in RSA. Then, for any m, $m \equiv m^{de} \pmod{N}$.

Comment. Using Euler's theorem, this follows immediately for residues m which are invertible modulo N. However, it then becomes tricky to argue what happens if m is a multiple of p or q.

Proof. By the CRT, we have $m \equiv m^{de} \pmod{N}$ if and only if $m \equiv m^{de} \pmod{p}$ and $m \equiv m^{de} \pmod{q}$.

Since $de \equiv 1 \pmod{(p-1)(q-1)}$, we also have $de \equiv 1 \pmod{p-1}$. By little Fermat, it follows that $m^{de} \equiv m \pmod{p}$ for all $m \not\equiv 0 \pmod{p}$. On the other hand, if $m \equiv 0 \pmod{p}$, then this is obviously true. Thus, $m \equiv m^{de} \pmod{p}$ for all m. Likewise, modulo q. □

Example 158. Bob's public RSA key is $N = 33$, $e = 3$.

(a) Encrypt the message $m = 4$ and send it to Bob.

(b) Determine Bob's secret private key d.

(c) You intercept the message $c = 31$ from Alice to Bob. Decrypt it using the secret key.

Solution.

(a) The ciphertext is $c = m^e \pmod{N}$. Here, $c \equiv 4^3 = 64 \equiv 31 \pmod{33}$. Hence, $c = 31$.

(b) $N = 3 \cdot 11$, so that $\phi(N) = 2 \cdot 10 = 20$.
To find d, we need to compute $e^{-1} \pmod{20}$. Since the numbers are so simple we see $3^{-1} \equiv 7 \pmod{20}$. Hence, $d = 7$.

(c) We need to compute $m = c^d \pmod{N}$, that is, $m = 31^7 \equiv (-2)^7 \equiv 4 \pmod{33}$.
That is, $m = 4$ (as we already knew from the first part).

Example 159. For his public RSA key, Bob needs to select p, q and e. Which of these must be chosen randomly?

Solution. The primes p and q must be chosen randomly. Anything that makes these primes more predictable, makes it easier for an attacker to get her hands on them [in which case, the secret key d is trivial to compute].

On the other hand, e does not need to be chosen at random. In fact, knowing any pair e, d such that $ed \equiv 1 \pmod{(p-1)(q-1)}$ would allow us to factor $N = pq$ (and thus break RSA). We'll prove that later.