MATH 4176 Notes

Kevin Lee

April 29, 2013

Jan 23rd

Diffie-Hellman Key agreement, AES

Jan 25th

Given $N = (pq)$

$M \to C = M^e (\mod N)$

$C \to C^d \equiv M^{de} \equiv M \mod N$

Euclidean GCD Algorithm + Extended Version

Def. Let $a, b \in \mathbb{Z}$ and let $a \neq 0$: we say $a|b$ (a divides b) provided there exists an integer c such that $b = ac$.
$a|b$ & $b|c = a|c$
$a|b$ & $b|a$, $a = \pm b$
$a|b$ and $a|c$ and $p, q \in \mathbb{Z} \to (a|pb + qc)$

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}, n \neq 0$. We say a is congruent to b mod n (written $a \equiv b (\mod n)$) provided $a - b$ is divisible by n (ie. $a - b = d * n, d \in \mathbb{Z}$).

Congruence mod n is an equiv relation:
$\forall a, b, c, n \neq 0, a \equiv a \mod n, a \equiv b \Rightarrow b \equiv a, a \equiv bb \equiv c \Rightarrow a \equiv c \mod n, a \equiv bc \equiv d \mod n \Rightarrow a \pm c \equiv b \pm d \mod n$

Common divisors

Let $a, b \in \mathbb{Z}$, d is a common divisor of a, b provided $d|a$ and $d|b$

Def. Let $a, b, \in \mathbb{Z} a, b \neq 0$, then g is a GCD of a and b provided g is a common divisor of a and b and g is the largest such common divisor.

Facts: g is a GCD of a and b if $g|a$ and $g|b$, $g > 0$, and if d is any common divisor of a and b then $d|g$

The GCD algorithm and its extension
Given $a, b \in \mathbb{Z}, b \neq 0$ there exists unique $g, r \in \mathbb{Z}, a = gb + r, 0 \leq r < b$.
If $d|a$ and $d|b$, then $d|a - qb$ so $d|r$.
If $d|b$ and $d|r$, then $d|qb + r$ so $d|a$.
$a = qb + r, a \leq r < b$, gcd(a,b) = gcd(b,r)
$\exists r_1 : b = q_1 r + r_1, 0 \leq r_1 < r$
$\exists r_2 : b = q_2 r_1 + r_2, 0 \leq r_2 < r_1$
$r > r_1 > r_2$
Last remainder = GCD

Ex. GCD of 118 and 267

Jan 28th

RSA Encryption Algorithm (Rivest, Shamir, Adelman)

How it works: Bob sets up the system. He chooses a large positive integer N (1024 bits) where $N = p * q$ and p and q are distinct primes about 512 bits each. He can then computes an integer $\phi(n) := a \in \mathbb{Z} | 1 \leq a \leq N, \gcd(a, N) = 1$. He chooses two integers e and d such that $e * d = 1 + k\phi(N)$ for some integer k. He then publishes both N and e (e is te encryption exponent). Bob keeps d, p, q, and $\phi(N)$ private.

Alice wants to send a message to Bob. She digitizes the message and breaks it into blocks, where each block = positive integer < N. Alice sends a block M by encrypting it: namely she computes $C \equiv M^e (\mod N)$ and sends it to Bob. (Recall: $a \equiv b \mod m$ means $a - b$ is a multiple of m, ie. $a = b + km$). Bob receives the message and decrypts it by computing $C^d = (M^e)^d \equiv M^{ed} \mod N$ and since $ed = 1 \mod \phi(N)$, $M^{ed} \equiv M \mod N$.

$\phi(pq) = (p-1)(q-1)$, if N can be factored, the system can be broken as $\phi(N)$ can be found. e is normally chosen for ease of computation (sparse, more 0s than 1s).

Euclidean Algorithm for computing GCD(a, b)

Euler-Fermat theorem: let m be a positive integer and let GCD$(a, m) = 1$ and $a^{\phi(m)} \equiv 1 \mod m$.

Jan 30th

Fast Multiplication/Exponentiation: known as double and add or square and multiply.

19	37
9	74
-4-	-148-
-2-	-296-
1	592
=	703

Binary representation of 19: 10011 = 16 + 2 + 1.
Binary reversed, add values under 1s:

1	1	0	0	1	
37	74	148	296	592	= 703

19 * 37 = 37 + 2*(37+2*2*2*37)

Cross out rows with even values on the left, add up remaining values on the right to get the product.

To multiply x by, say, 19: (go from left to right)

1	0	0	1	1
1x	2x	4x	8x	18x
1x			9x	19x

To multiply x by, say, 112:

1	1	1	0	0	0	0
	2x	6x	14x	28x	56x	112x
x	3x	7x				

To calculate x^{53}, 53 = 110101

1	1	0	1	0	1	
x	x^2	x^6	x^{12}	x^{26}	x^{52}	Answer
x	x^3		x^{13}		x^{53}	Mult

Shift left and add one if the bit is 1. To find x^{545} takes 9 squaring and 2 multiplications.

Feb 1st

Chinese Remainder Theorem

Let $m_1, ..., m_n$ be pairwise relatively prime positive integers and let $q_1, ..., q_n$ be integers. Then the system of congruences $x \equiv q_1 \mod m_1, ..., q_n \mod m_n$ has a solution which is unique mod $(m_1, ..., m_n)$.

Proof: Let $M = m_1, ..., m_n$. For $1 \leq j \leq n_i$ let $M_j = \frac{M}{m_j}$

Claim: If $1 \leq i \leq n$, then ... (see book)

Feb 4th

Recall n be a positive integer and let $a \in \mathbb{Z}^+$ with $\gcd(a, n) = 1$ (standard hypothesis)

If $e * d \equiv 1 \mod (p-1)(q-1)$, then $(M^e)^d \equiv M \mod pq$ (based on Euler-Fermat Theorem)

Def. Given the standard hypothesis, the order of $a \mod n$ written $\text{ord}_n a$ is the least possible r such that $a^r \equiv 1 \mod n$ if it exists.

Theorem. Given the standard hypothesis, $\text{ord}_n a$ does exist.

Proof. Write down powers of $a \mod n$: $a, a^2, a^3, ... \mod n$
Ex. Powers of 3 mod 23: 3, 9, 14, 12, 13, 15, 2, 6, 18, 8, 1, 3, 9, ... repeats! (pigeon hole principle (PHP))
By PHP, after at most n+1 steps, the powers repeat.
Let $i < j$ and let $a^i \equiv a^j \mod n$.
Ex. $5^8 \equiv 5^{38} \mod 31$. 5^8 has one inverse mod 31 so $5^{-8} * 5^8 \equiv 5^{-8} * 5^{38} \mod 31, 1 \equiv 5^{30} \mod 31$

Because gcd(a,n)=1, it follows that a is invertible mod n (recall the affine cipher). If a^* satisfies $a^*a \equiv 1 \mod n$, then $(a^*)^i a^i \equiv (a^*)^i a^j \mod n$. $\therefore 1 \equiv a^{-i}a^j \equiv a^{j-i} \mod n$ and $j - i > 0$. Thus r exists and the least such positive number is the order.

Last time - looked at $\text{ord}_7 a$ for $1 \leq a \leq 6$.

a	1	2	3	4	5	6
$\text{ord}_7 a$	1	3	6	3	6	2

For all a, $\gcd(a, 7) = 1$, $\text{ord}_7 a$ is a divisor of 6.

n = 8

a	1	3	5	7
$\text{a}_8 a$	1	2	2	2

n = 9

a	1	2	4	5	7	8
$\text{a}_9 a$	1	6	3	6	3	2

What you notice is that the number of possible values of a's is related to the order

Def. Let n be a positive integer. Define $\phi(n) = \#$ of positive integers such that $1 \leq a \leq n$ and $\gcd(a, n) = 1$. $\phi(n)$ is called the Euler-Phi function (EulerPhi[n] in Mathematica).

For p a prime: $\phi(p) = p - 1$.
q another prime, $q \neq p$. $\phi(pq) = pq - q - p + 1$; throwing away $(p, 2p, ..., (q-1)p, qp)$ and $(q, 2q, ..., (p-1)q, pq)$ but leaving one pq. $\phi(pq) = pq - q - p + 1$ then factors into $\phi(pq) = (p-1)(q-1)$.

$\phi(p^3) = p^3 - p^2 = p^2(p-1) = p^3(1 - \frac{1}{p})$; throwing away $(p, 2p, ..., (p^2-1)p, p^2p)$

Feb 6th

Let $\gcd(a, n) = 1$; $n > 1$ such that $a^k \equiv 1 \mod n$

Given such n and a, $\text{ord}_n a$ exists (proof by PHP, any string of n+1 consecutive powers of a mod n must have a repeated number. If $a^i \equiv a^j \mod n$ with $i < j$, then $a^{j-i} \equiv a^i(a^j)^{-1}$ with $j - i > 0$.

We looked at powers of 3 mod 23: ....

Fermat's Little Theorem: Let p be a prime and get $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \mod p$.

Feb 8th

Proof: if gcd(a,n) = 1 and $a^k \equiv 1 \mod n$ then $\text{ord}_n a$ divides k.

Suppose $a^k \equiv 1 \mod n$. Let $k = q{*}\text{ord}_n(a) + r$ with $0 \le r <\text{ord}_n(a)$

Show $r = 0$ by def and by assumption, $1 \equiv a^k \equiv a^{q*ord_n(a)+r} \equiv (a^{ord_n(a)})^q * a^r \mod n \equiv a^r \mod n$.

Thus $a^r \equiv 1 \mod n, 0 \le r < ord_n(a)$ and so $r = 0 \therefore k$ is a multiple of $\text{ord}_n(a)$.

Cor. Since $a^{\phi(n)} \equiv 1 \mod n$ by Euler-Fermat theorem, it follows that $\text{ord}_n(a)|\phi(n)$.

Def: primitive element: let p be a prime. A primitive element mod p is an integer α such that α has order $p-1$ mod p.

Assumption: every prime has a primitive element.

Given ϕ and α, a primitive element mod p. Solve $\alpha^k \equiv \beta \mod p$ where β is given.

The mapping of $\mathbb{Z}_p^*$ to $\mathbb{Z}_p^*$ by $k \to \alpha^k \mod p$ is 1-1 and onto.

Nice theorem (5.8): Let p be a prime > 2 and let $\alpha \in \mathbb{Z}_p^*$. Then α is a primitive element mod p if and only if for each prime divisor q of $p-1$, $\alpha^q \not\equiv 1 \mod p$.

Proof: Let α be a primitive and let q be a divisor of $p-1$. α primitive $\Rightarrow \text{ord}_p(\alpha) = p-1$. Since $q|p-1$ and q is a prime, we have that $1 < q \le p-1$ and $1 \le \frac{p-1}{q} < p-q$. By def of $\text{ord}_p(\alpha)$, $\alpha^{\frac{p-1}{q}} \not\equiv 1 \mod p$.$[\frac{p-1}{q} \ge 1$ and $\frac{p-1}{q} <\text{ord}_p(\alpha)]$

Suppose α is not primitive. Let $\text{ord}_p(\alpha) = i < p-1$. $1 \le i < p-1$; $\frac{p-1}{i}$ is an integer ≥ 2.

Let q be a prime divisor of $\frac{p-1}{i}$. Then q is a prime divisor of $p-1$. So $\frac{p-1}{i} = qd$ for some integer d. So $\frac{p-1}{q} = di$. Then $\alpha^{\frac{p-1}{q}} = \alpha^{di} \equiv (\alpha^i)^d = (\alpha^{ord_p \alpha})^d \equiv 1 \mod p$.

Feb 11th

$p = 2q+1$ where q is a odd prime. p is called a SophieGermain prime. Given $\alpha \not\equiv \pm 1 \mod p$. Prove that α is a primitive element if and only if $a^q \equiv -1 \mod p$.

Use the Nice theorem (5.8). Let $p-1 = q_1, ..., q_r$. Then α is a primitive element mod p if and only if $\{\alpha^{\frac{p-1}{q_1}}, ..., \alpha^{\frac{p-1}{q_r}}\}$ contains no occurrences of 1 (mod p). We see that $p-1 = 2q$, so the list of prime divisors of $p-1$ is $\{2, q\}$. Consider $\alpha^{\frac{p-1}{q}} \mod p$. By def, $\frac{p-1}{q} = 2$, so we test $\alpha^2 \mod p$. Is $\alpha^2 \equiv 1 \mod p$? No. For p is a prime and if $\alpha^2 \equiv 1 \mod p$, then $(\alpha-1)(\alpha+1) \equiv 0 \mod p \Rightarrow p|(\alpha-1)(\alpha+1) \Rightarrow p|(\alpha-1)$ or $p|(\alpha+1) \Rightarrow \alpha \equiv 1$ or $-1 \mod p$. Therefore by the N.T., α is a primitive if and only if $\alpha^{\frac{p-1}{2}} = \alpha^q \not\equiv 1 \mod p$. But $\alpha^{\frac{p-1}{2}} = \alpha^{p-1} \equiv 1 \mod p$. Therefore $(a^q)^2 \equiv 1 \mod p \Rightarrow \alpha^q \equiv \pm 1 \mod p$. Therefore α is a prime if and only if $\alpha^q \equiv -1 \mod p$.

$n = pq, \phi(n)$ is known, $\phi(pq) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$. $p + q = n + 1 - \phi(n)$. $\Rightarrow p^2 + (\phi(n) - n - 1)p + n = 0$

RSA: Given p and q large primes and exponents e and d, to encrypt: $M \to M^e \mod n$. To decrypt: $C \to C^d \equiv 1 \mod n$.

The idea is that p and q are private, $n = pq$ is public, d is private, e is public. Knowing p and q, one cna compute $\phi(n)$, from ehich one can compute d, where $ed \equiv 1 \mod \phi(n)$. Thus $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{k*\phi(n)+1} \equiv (M^{\phi(n)})^k * M \mod n$. By EulerFermat, $\equiv 1^k M = M \mod n$.

Issues: how to choose p, q, e.

The Monte Carlo algorithm - A yes-biased M.C algorithm is a randomized based algorithm for a decision problem such that a YES answer is correct and a NO answer may be correct.

The Las Vegas algorithm - a random algorithm for a decision problem which may not give an answer. But if it does, it is correct.

Tools for testing for primility

- The decision problem is called COMP(OSITE)
- Algorithms are yes-biased M.C

A yes-biased M.C has an error problem of ϵ y, in an instance in which the answer is "yes", the algorithm gives the (wrong) answer NO with probability $\leq \epsilon$.

FLT If n is a prime and gcd(a,n) =1, then $a^{n-1} \equiv 1 \mod n$.

Contrapositive: $a^{n-1} \not\equiv \mod n \Rightarrow$ n composite.

Feb 13

$a^{p-1} \equiv 1 \mod p$ for all a, $(a,p) = 1$ where p is a prime

If $p - 1 = q_1, ..., q_k$ and a satisfies $a^{\frac{p-1}{q_1}} \not\equiv 1 \mod p$ for $1 \leq i \leq k$, then a is a prime.

$p = 2q + 1, p - 1 = 2q$. Want a to satisfy $a^{\frac{p-1}{2}} \not\equiv 1$ and $a^{\frac{p-1}{q}} \not\equiv 1 \mod p$. $a^{\frac{p-1}{2}} \equiv a^q$? and $a^{\frac{p-1}{q}} \equiv a^2$?

$a \not\equiv 1 \mod p$ so $a^2 \not\equiv 1 \mod p$.

If a is primitive, $a^q \not\equiv 1 \mod p$. $a^q \equiv a^{\frac{p-1}{2}} \mod p$ so $(a^q)^2 \equiv a^{p-1} \equiv 1 \mod p$. Therefore $a^q \equiv 1$ or -1 mod p.

$\phi(n) = pq - (p+q) + 1$, so $p + q = pq + 1 - \phi(n)$. $q = n/p$ so $p + \frac{n}{p} = n + 1 - \phi(n) \Rightarrow p^2 + n = (n + 1 - \phi(n))p$.

FLT: If n is prime and gcd(a,n)=1, then $a^{n-1} \equiv 1 \mod n$.

Contrapositive: If gcd(a,n)=1 and $a^{n-1} \not\equiv 1 \mod n$, then n is a composite.

Compositeness Test: yes-biased Monte-Carlo. Is n a composite?

Randomly pick a such that gcd(a,n)=1. Compute $a^{n-1} - 1 \mod n$. If $a^{n-1} - 1 \not\equiv 0 \mod n$ return yes, else return no.

Pseudo-primes (impostor:) $a = 2, n = 341 = 11 * 31$. However, $2^{10} \equiv 1 \mod 11$ by FLT for 11(*). Also, $2^5 = 32 \equiv 1 \mod 31$. Therefore $2^{10} \equiv 1 \mod 31$. (**)

The system (*) and (**) of congruences has a unique solution mod 341. Thus $2^{10} \equiv 1 \mod 341$ therefore $1 \equiv (2^{10})^{34} \equiv 2^{340} \mod 341$!!

Def. Let n be an integer > 1, and let gcd(a,n) = 1. Then we call a a pseudo prime to base b if b is an integer that satisfies $b^{n-1} \equiv 1 \mod n$ and n is a composite. [n is a pseudo prime to base b]

So 341 is a pseudo prime to base 2. What about $b = 3$? $3^5 \equiv 3^{10} \equiv 1 \mod 11$ (FLT). $3^{10} \equiv 25 \mod 31$. Now $3^{30} \equiv 1 \mod 31$ (FLT). Thus $(3^{10})^{33} \equiv 1^{33} \equiv 1 \mod 11 \equiv 1 \mod 31$. Then $3^{330} \equiv 1 \mod 341$. Therefore $3^{330} \equiv 3^{330} * 3^{10} \equiv 25 \mod 341$. Therefore 341 is a composite.

However! There are universal pseudo primes that fail all tests of compositeness. There exists numbers n for which n is composite and yet for every b with gcd(b,n) = 1, $b^{n-1} \equiv 1 \mod n$. n is a pseudo prime (x) if gcd(x,n) = 1 and $x^{n-1} \equiv 1 \mod n$.

ie. $x^{n-1} - 1 \equiv 0 \mod n$.

Suppose $x^{n-1} - 1 = f_1(x) f_2(x) ... f_r(x) \mod n$

If n is a prime and $n | x^{n-1} - 1$, then $n | f_1(x)$ or $n | f_2(x)$ or ... or $n | f_r(x)$.

$2^{340} - 1 = (2^{170} + 1)(2^{170} - 1) = (2^{170})(2^{85} + 1)(2^{85} - 1) \equiv 0 \mod 341$. But $2^{170} \equiv 2 \mod 341$; $2^{85} + 1 \equiv 2 \mod 341$; $2^{85} - 1 \equiv 33 \mod 341$. Correct factorization next time.

Example: $n = 561 = 3 * 11 * 17$. gcd(b,n) $= 1 \Rightarrow b^{560} \equiv 1 \mod 561$.

Feb 15th

More about primality and compositeness

n is a pseudo prime to base b [psp(b)], if $b^{n-1} \equiv 1 \mod n$ and n is a composite, FLT: if $\exists b : b^{n-1} \not\equiv 1 \mod n$ and (b,n) = 1, then n is a composite.

$2^{340} \equiv 1 \mod 341$ and 341 = 11*31

$3^{340} \not\equiv 1 \mod 341 \Rightarrow 341$ composite.

$b^{n-1} \equiv 1 \mod n$ means $b^{n-1} - 1$ is divisible by n.

See: write $n-1 = 2^k m$, with m odd. Then $a^{n-1} - 1 = a^{2^k * m} - 1 = (a^{2^{k-1}m} + 1)(a^{2^{k-2}m} + 1)...(a^{2m} + 1)(a^m + 1)(a^m - 1)$

If n is a prime, and $n | a^{n-1}$, then n must divide one of the factors over the RHS.

Yes Test for decision problem: n is composite: Factor $n - 1 = 2^k m$, with k is a positive integer and m odd. Randomly choose a with gcd(a,n)=1. Set $b := a^m$. If $b \equiv 1 \mod n$, return ("n is prime') [No, n is not a composite]. else for $i = 1$ to $k - 1$, do the following:

If $b \equiv -1 \mod n$ return ('n is prime'); else $b := b^2$ endif. and for ; return ('n is composite')

Miller-Rabin Test (above)

Thm. M-R is a yes-biased test for compositeness.

Proof 1: Suppose the M-R test returns yes. This is impossible if n is a prime. (work backwards in the algorithm)

Fact: If n is prime and $x^2 \equiv 1 \mod n$, then $x \equiv 1$ or $x \equiv -1 \mod n$.

Suppose n is a prime, let a be an integer rel. prime to n. Then $a^{n-1} = a^{2^k m} \equiv 1 \mod n \Rightarrow (a^{2^{k-1}m})^2 \equiv 1 \mod n$. But $a^{2^{k-1}m} \not\equiv -1$(else $\rightarrow$ NO). Therefore $a^{2^{k-1}m} \equiv 1 \mod n$. Thus $1 \equiv (a^{2^{k-2}m})^2 \mod n$. No stop so $a^{2^{k-2}m} \equiv 1 \mod n$ Continue in this way to $(a^m)^2 \equiv 1 \mod n$. Therefore $a^m \equiv \pm 1 \mod n$ which would have returned No.

Def. If gcd(b,n) = 1, n failes the M-R test (ie. test yields prime) and yet n is composite, we call n a string pseudo prime to base b "spsp(b)".

Ex. $M := 2^n - 1 = 24 * 89$ If $2^n - 1$ is prime, then n is prime.

Feb 18th

11213 * 104369 = 11703... (11212 * 104368 = 11702...) note that the first few digits are identical. p, q 10^{50}, $p * q = 10^{100}$, $\phi(pq) = pq - p - q + 1 = n - (p + q - 1)$ thus we know that there is a finite number of solutions. Find a factor of $de - 1$ that has the same length as N.

The integer factoring problem.

Classes of factoring methods

1. BFI: brute force and ignorance
2. Birthday match techniques
3. Using FLT and generalizations
4. Combination of congruences: If $p|(x-y)(x+y)$ then $p|x-y$ or $p|x+y$. The idea is to find two squares $X^2 and Y^2$ such that $X^2 \equiv Y^2 \mod N$ but $X \not\equiv Y \mod N$. (Fermat)

Pollard's p-1 algorithm 1974:

1. Let α be an integer $\neq \pm 1$ and $\text{GCD}(\alpha, N) = 1$
2. Raise α to a very large power $B \mod N$.

If p is a prime divisor of N (GCD$(\alpha, p) = 1$)and $p-1|B$, then $\alpha^B \equiv 1 \mod p$. Therefore $\alpha^B - 1 \equiv 0 \mod p$. Then GCD$(\alpha^B - 1, N)$ is a multiple of p.

What has to happen for this to work? $N = 488533, \alpha = 2, B = 20!$; $B = 2 * 3 * ... * 19 * 20$ so happens that $456 = 2^3 * 3 * 19|20!$ and $457 * 1069 = N$.

Feb 20th

Pollard p-1: Let N be a large composite number. If N has a prime factor p such that all prime power factors of $p-1$ are $\leq M$, where M is suitably chosen then the number $\alpha^M - 1$ for $\alpha \neq \pm 1$, GCD$(\alpha, N) = 1$ will be divisible by p.

If GCD$(\alpha, N) = 1$, then GCD$(\alpha, p) = 1$ for each prime divisor p of N. If $p-1|M$, then

1. $\alpha^{p-1} \equiv 1 \mod p$ (by FLT)
2. $\alpha^M \equiv 1 \mod p$ ($\text{ord}_p \alpha | p-1$ and $p-1|M$)
3. $\therefore p | \alpha^M - 1$
4. $\therefore p | \text{GCD}(\alpha^M - 1, N)$

$p-1$ algorithm: pick some value of B, an integer that's "big enough but not too big". [$B!$ is going to be over value of M]

Find $\alpha^{B!} \mod N$ ans $= \alpha$ for [$i = 0$;$i \leq B$;i++] ans := ans^i mod N g = GCD[ans-1,N] if g$\neq$1 or N, stop. else keep going

PollardRho: Let $N = pq$. Iterate a random function f on $\mathbb{Z}_N \to \mathbb{Z}_N$.

Ex. $f(x) = x^2 + 1 \mod N$, $f'(x) = f(x), f^2(x) = f \circ f(x), f^{n+1}(x) = f \circ f^n(x)$...

To factor $N = pq$, generate two sequences: $x_0 = 1$, $x_1 = f(x_0) = z; y_1 = f(f(x_2)) = 5$

Feb 22nd

We know that if n is a prime > 2 and $x \in \mathbb{Z}$, then $x^2 \equiv 1 \mod n \Rightarrow x \equiv \pm 1 \mod n$.

Note that if $a^{\frac{n-1}{2}} \mod n$, where $\gcd(a, n) = 1$, then $y^2 \equiv (a^{\frac{n-1}{2}})^2 \equiv a^{n-1} \equiv 1 \mod n$ (by FLT)

Therefore if $\gcd(a, n) = 1$ and n is an odd prime, then $a^{\frac{n-1}{2}} \equiv \pm 1 \mod n$.

Consequences: Euler's criterion: If n is an odd prime and $\gcd(a, n) = 1$, then $a^{\frac{n-1}{2}} \equiv 1$ or $-1 \mod n$.

Def. If p is an odd prime, and $\gcd(a, p) = 1$, if there exists a solution x such that $x^2 \equiv a \mod p$ has a solution, then we say that x is a quadratic residue (QR) mod p and x is a quadratic non-residue (QNR) otherwise.

The squares mod 13: Squares: $1, 4, 9, 16 \equiv 3, 25 \equiv 12, 36 \equiv 10$, Non squares: $2, 5, 6, 7, 8, 11$

The powers of 2 mod 13:

k	1	2	3	4	5	6	7	8	9	10	11	12
2^k mod 13	2	4	8	3	6	12	11	9	5	10	7	1
nonsq:	2		8		6		11		5		7	
	2		2^3		2^5		2^7		2^9		2^{11}	
sq:		4		3		12		9		10		1
		2^2		2^4		2^6		2^8		2^{10}		2^{12}

Euler's Criteron Reinvented: Let p be an odd prime. Then a is a QR mod p if and only if $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

Proof. If a is a QR mod p, then there exists b such that $a \equiv b^2 \mod p$. Thus $a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \mod p$ (by FLT)

Suppose $a^{\frac{p-1}{2}} \equiv 1 \mod p$. Let g be a primitive element mod p. That is $\{g, g^2, ..., g^{p-1}\} \equiv \{1, 2, ..., p-1\}$ mod p in some order. Therefore we may write $a = g^k$ for some integer k. Then $1 \equiv a^{\frac{p-1}{2}} \equiv g^{\frac{k(p-1)}{2}} \mod p$. Thus $p-1|\frac{k(p-1)}{2}$, so $\frac{k}{2}$ is an integer. $\frac{k}{2} = l, k = 2l$, and so $a = g^{2l} = (g^l)^2$ is a QR mod p.

Some notation: Let p be an odd prime and let $a \in \mathbb{Z}$. Define the Legendre symbol $(\frac{a}{p})$ "a over p" by $(\frac{a}{p}) = \{$ 0 if $p|a$, 1 if $\gcd(a,p) = 1$ and $x^2 \equiv a \mod p$ has a solution [a is a QR mod p], -1 otherwise }

Euler's Criteron (Final): If p is an odd prime and $\gcd(a,p) = 1$, then $a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \mod p$

A question: suppose n is an odd integer and $\gcd(a,n) = 1$, and $a^{\frac{n-1}{2}} \equiv (\frac{a}{n}) \mod n$. Does that imply that n is a prime?

The Solovary-Strassen compositeness test: pick $\alpha, 1 < \alpha < n$, at random. If $\gcd(a,n) \neq 1$, return composite. Else $x = (\frac{a}{n})$. Set $y = a^{\frac{n-1}{2}} \mod n$. If $x \equiv y \mod n$ return prime. else return composite.

Feb 25th

Midterm 1: Bring paper!

Topics: Overview PKC, XGCD, RSA, Monto Carlo and Las Vegas Test, Square and Multiply, Issues with RSA, CRT, Z_n^* (set of numbers invertible mod n), FLT, Euler-Fermat, $\phi(n)$, orders of elements ($\text{ord}_n(a)$), primeality testing (finding primes), primitive elements, certificates of primitivity, why RSA is hard to break, pseudoprimes, psuedoprime test (if $a^{n-1} \equiv 1 \mod n$, return PRIME, else return COMPOSITE), strong pseudoprimes, Miller-Rabin Test ($n-1 = 2^e * t$, t odd, if n is prime, then n divides one of the factors of $\alpha^{n-1} - 1 = (\alpha^t - 1)(\alpha^t + 1)(a^{2t+1})....(a^{2^{e-1}t} + 1)$), Factoring, Pollard $p-1$, Pollard Rho

Given p a prime > 2, and $a \in \mathbb{Z}$, define $(\frac{a}{p})$ by ...

Euler's Criteron: If $\gcd(a,p) = 1$, then $a^{\frac{p-1}{n}} \equiv 1$ or -1 where a is a QR mod p or a QNR mod p respectively.

Showed that if g is a prime elt mod p and $a \equiv g^k \mod p$, then a is a square mod p if and only if k is even.

Euler's Criteron showed that if p is an odd prime and gcd(a,p) = 1, then $a^{\frac{o-1}{2}} \equiv (\frac{a}{p}) \mod p$

Solovay-Strassen Test (yes-biased for "n is composite") For random a, calculate $a^{\frac{n-1}{2}}$ and $(\frac{a}{n})$. If they are equal, return prime. else return composite.

Ex. Find $(\frac{7411}{9283})$ In Mathematica, use JacobiSymbol[7411,9283].

Let n be odd and positive. Thus, $n = p_1^{e_1}...p_r^{e_r}$, p_i all odd. Let $a \in \mathbb{Z}$, then define the Jacobi Symbol $(\frac{a}{n}) := \prod_{i=1}^{r} (\frac{a}{p_i})^{e_i}$

Rules - Let $a, b \in \mathbb{Z}$ and n an odd and positive. Then:

1. If $a \equiv b \mod n$, then $(\frac{a}{n}) = (\frac{b}{n})$
2. $(\frac{2}{n}) = 1$ if $n \equiv 1$ or $-1 \mod 8$, -1 if $n \equiv 3$ or $-3 \mod 8$
3. $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$
4. QRL: If m and n are odd positive integers and gcd(m,n) = 1, then $(\frac{m}{n}) = (\frac{n}{m})$ if $n \equiv 1 orm \equiv 1 \mod 4$

Mar 1st

Chapter 6!

Discrete log problem mod p: given a prime p, a primitive element g mod p and an integer β, we know there exists $l \in \{1, 2, ..., p-1\}$ such that $g^l \equiv B \mod p$ given g and β, find l.

Given $b^x = y$ where $b, y \in \mathbb{R}^+$ then $x\ln(b) = \ln(y)$ so $x = \frac{\ln(y)}{\ln(b)}$

Cant do this with mods!

Mod 13: $g = 2$. by log y is meant the number l such that $2^l \equiv y \mod \beta$

l	1	2	3	4	5	6	7	8	9	10	11	12
$2^l \mod 13$	2	4	8	3	6	12	11	9	5	10	7	1

Rearrange $2^l \mod 13$ to invert permutation

$2^l \mod 13$	1	2	3	4	5	6	7	8	9	10	11	12
l	12	1	4	2	9	5	11	3	8	10	7	6

primitive element is called a generator in modern algebra

For moderately large prime, the permutation of logs is hard to determine.

Alice — Bob

Public Key: P a large prime, g and a primitive element mod P.

Private Information: integer mod $P - 1$

Alice picks α, Bob picks β

Alice computes g^α mod P, calls this A

Bob computes g^β mod P, calls this B

Alice sends A to Bob, Bob sends B to Alice

Bob computes B^α. Alice computes A^β

Since $B^\alpha = (g^\beta)^\alpha \equiv g^{\beta\alpha} \equiv (g^\alpha)^\beta = A^\beta \mod P$

Thus Alice and Bob have a shared secret number.

March 4th

El Gamul crypto system - Discrete logs in a general setting

G is a finite group under multiplication such as $\mathbb{Z}_p^*$

$\alpha \in G$ has order n where n is the smallest positive integer k such that $\alpha^k = 1$ where 1 is the identity el't of G.

Given discrete log problem in G: given β known to be a power of α, find the power. That is, given α and $\beta = \alpha^l$, find l.

Define $< \alpha >= \{\alpha^k : 0 \leq k \leq n-1\}$ where $n =$ order of α. Given $\beta \in < \alpha >$, find the unique $l \in \{0, 1, ..., n-1\}$ such that $\beta = \alpha^l$.

The El Gamal cryptosystem.

Alice — [Eve] — Bob

Alice sends message to Bob

Public Info: takes place in $\mathbb{Z}_p^*$, the non-zero integer mod p (large prime). The public information is then prime p and a primitive element α mod p ($\alpha \in \mathbb{Z}_p^*$, and $< \alpha >= \{\alpha^j : 0 \leq j \leq p-1\} = \mathbb{Z}_p^*$)

Bob chooses some random integer $a \in \{1, ..., p-1\}$ and computes $\beta \equiv \alpha^a$ mod p. Bob keeps a secret and publishes β.

Thus the public information (key) is p, α, β. Bob's private info is a. Alice's private info is a randomly chosen integer $k \in \{1, ..., p-1\}$.

To send a message X, Alice computes $y_1 \equiv \alpha^k \mod p$ and $y_2 = X \times \beta^k \mod p$.

Alice sends the pair (y_1, y_2) to Bob.

To read the message, Bob knows that $y_2 = X \times \beta^k$ and $\beta = \alpha^a$. Thus $y_2 = X \times \beta^k \equiv X \times (\alpha^a)^k \equiv X \times (\alpha^k)^a \equiv X \times y_1^a$.

Because Bob knows a, $X \equiv y_2 \times (y_1^a)^{-1} \mod p$ for $y_2 \times (y_1^a)^{-1} = X \times y_1^a \times (y_1^a)^{-1} = X \mod p$. Thus Bob knows X.

If Eve can compute discrete log mod p, then Eve can read the message.

Do not reuse α or k but a can be reused.

Attacks on the discrete log problem

Shanks Algorithm (also known as "baby step giant step") is for solving the discrete log problem.

Given α, β, where $\beta = \alpha^l$, ord(α) = n, and $0 \leq l \leq n-1$

All in a group G where α has an order n.

Set $m =$ ceiling $\ulcorner \sqrt{n} \urcorner$ = least integer $\geq \sqrt{n}$. (ceiling(300) = 18)

Stinson uses $\ulcorner \sqrt{n} \urcorner = m$

From two lists of ordered pairs:

1. $L_1 = \{(j, \alpha^{mj}) : 0 \leq j \leq m-1\}$
2. $L_2 = \{(i, \beta\alpha^{-i}) : 0 \leq i \leq m-1\}$

$0 \leq l = \log_\alpha \beta \leq n-1$

Divide l by m to get $l = q_1 m + q_0$ with $0 \leq q_0 \leq m-1$ and $0 \leq l \leq n-1$. $m \geq \sqrt{n} \Rightarrow m^2 \geq n$ so $0 \leq m-1 \leq m^2-1 = m^2-m+m-1 = m(m-1)+m-1$

March 8th

Pollard-Rho for DLP (given $\beta \in G$, find $l : \beta = \alpha^l$ in G)

Setup: a group G - cyclic of order n ($\exists \alpha \in G : G = \{\alpha, \alpha^2, ..., \alpha^n\} = <\alpha>$)

1. Partition G into roughly 3 equal sized subsets s_1, s_2, s_3.
2. Define a function of 3 variables

   $f(x, a, b) = (\beta x, a, b+1)$ if $x \in s_1$

   $f(x, a, b) = (x^2, 2a, 2b)$ if $x \in s_2$

   $f(x, a, b) = (\alpha x, a+1, b)$ if $x \in s_3$

   Begin at (1,0,0)

Particular example: $G = \mathbb{Z}_p^*$

$s_1 = \{x : x \equiv 1 \mod 3\}$ $s_1 = \{x : x \equiv 0 \mod 3\}$ $s_1 = \{x : x \equiv 2 \mod 3\}$

Thus $f(1, 0, 0) = (\beta, 0, 1)$

Additional rule: Each triple must satisfy $x = \alpha^a \beta^b$

if (x, a, b) satisfies $x = \alpha^a \beta^b$, then $f(x, a, b) = (x_1, a_1, b_1)$ satisfies $x_1 = \alpha^{a_1}\beta^{b_1}$

$x \in s_1 \Rightarrow (x_1, a_1, b_1) = (B_x, a, b+1)$ and $x = \alpha^a\beta^b \Rightarrow x_1 = \beta x = \alpha^a \beta^{b+1}$

if $x = \alpha^a\beta^b$ and $x \in s_2$, then $x_1 = x^2 = \alpha^{2a}\beta^{2b}$ and $f(x, a, b) = (x^2, 2a, 2b)$ and same with s_3

—

Compute $(x_1, a_1, b_1)(x_2, a_2, b_2), ..., (x_k, a_k, b_k)$ and $(x_2, a_2, b_2)(x_4, a_4, b_4), ..., (x_{2k}, a_{2k}, b_{2k})$

Check to see if $x_k = x_{2k}$, then $\alpha^{a_{2k}}\beta^{b_{2k}} = \alpha^{a_k}\beta^{b_k}$.

Let $\beta = \alpha^l$ (l is the unknown DL of β) and so $\alpha^{a_{2k}}\alpha^{lb_{2k}} = \alpha^{a_k}\alpha^{lb_k}$. Therefore $\alpha^{a_{2k}+lb_{2k}} = \alpha^{a_k+lb_k} \Rightarrow \alpha^{a_{2k}-a_k+l(b_{2k}-b_k)} = 1$

If $\alpha^r = 1$, then $\text{ord}_\alpha | r$. Therefore $a_{2k} - a_k + l(b_{2k} - b_k) \equiv 0 \mod n$, where n = ord α

If GCD$(b_{2k} - b_k, n) = 1$, then $l \equiv (b_{2k} - b_k)^{-1}(a_k - a_{2k}) \mod n$

The Birthday paradox

Let P_k = Prob(no two out of k share a birthday)

$P_2 = \frac{364}{365}$, $P_3 = \frac{364}{365}\frac{363}{365}, \ldots$

Pr(at least on birthday match) $= 1 - \prod_{i-1}^{k-1}(1 - \frac{i}{365})$

Plotted, point of inflection is at 23

March 18th

The discrete log problem (DLP): Given a group G (multiplicative for now) and $\alpha \in G; \beta \in G$ satisfies $\beta \in <\alpha> := \{\alpha^k | k \in \mathbb{Z}\}$

Since $\beta \in <\alpha>$, there exists l such that $\beta = \alpha^l$. DLP: find l : log β

Specialize to $\mathbb{Z}_p^*$, which has a primitive element α whos order = p - 1 and so if $\alpha^l \equiv \beta \mod p$, then $l \in \{2, ..., p-2\}$

The Index Calculus - fast attack on discrete logs

But first: Factoring by combining congruences.

Begins with Fermat's observation:

$n = x^2 - y^2 = (x-y)(x+y)$, find x and y such that $x^2 - y^2 = n$, with $n = (x-y)(x+y)$ with $x \pm y \neq 1$ or n.

Guess?: suffices to find x and y: $x^2 \equiv y^2 \mod n$ $[x^2 - y^2 = n * k]$ but $x \not\equiv \pm y \mod n$ then $\gcd(x - y, n)$ is a proper factor of n.

March 20th

Factoring using squares (see handout)

March 22nd

The Index Calculus

Index calculus for discrete logs in $\mathbb{Z}_p^*$

Given $\alpha, \beta \in \mathbb{Z}_p^*$ where α is a primitive element and there exists an integer l where $(1 \leq l \leq p-1)$ such that $\beta \equiv \alpha^l \mod p$. Find l.

Two phases:

1. Pre-computation: Pick a set $B = \{p_1, p_2, ..., p_B\}$ of small primes. Let $C \sim |B| + 10 = B + 10$. Find about C congruences mod p, each of the form $\alpha^{xj} \equiv p_1^{e_{1,j}} p_2^{e_{2,j}} ... p_B^{e_{B,j}} \mod p$ where e_i is an integer ≥ 0.

   Lemma: If $l_1 = \log \beta_1$ and $l_2 = \log \beta_2$, then $\log(\beta_1\beta_2) \equiv l_1 + l_2 \mod p-1$.

   Proof: Let $l = \log \beta_1\beta_2$. Then $\alpha^l = \beta_1\beta_2 \equiv \alpha^{l_1}\alpha^{l_2} \equiv \alpha^{l_1 l_2} \mod p \Rightarrow l \equiv l_1 + l_2 \mod p-1$

   Each of these C congruences can be written as $xj = e_{1,j}p_1 + e_{2,j}p_2 + ... + e_{B,j}p_B \mod p-1$

Try to solve the system of congruences $x_1 \equiv e_{1,1}p_1 + ... e_{B,1}p_B \mod p-1$ ... $x_C \equiv e_{1,C}p_1 + ... + e_{b,C}p_B \mod p-1$

This yields $\{\log p_1, \log p_2, ..., \log p_B\}$

2. Computation phase: pick random values of $s \in \{1, ..., p-1\}$

   Compute $\gamma \equiv \beta\alpha^s \mod p$ and hope that you can factor γ over B

   If it works for some s for which $\log(\beta\alpha^s) = r_1 \log p_1 + ... + r_B \log p_B \mod p-1$, you have $\log\beta + s\log\alpha \equiv r_1 \log p_1 + ... + r_B \log p_B \mod p-1$

   $\Rightarrow \log\beta = \sum_{i=1}^{B} r_1 \log p_i - s \mod p-1.$

   $\log\beta = l$ means $\beta = \alpha^l$. Therefore $\log\alpha = l$ means $\alpha^1 = \alpha^l$.

A tiny but useful example: $p = 131, \alpha = 2$. Find $\log 37$, that is the value of l such that $37 \equiv 2^l \mod 131$.

let $B = \{2, 3, 5, 7\}$. $\log n = \log_2 n \mod p$

$\log 2 = 1$ because we know $2^1 = 2$.

$2^8 \equiv 5^3 \mod p, 2^{12} \equiv 5 * 7, 2^{14} \equiv 3^2, 2^{34 \equiv} 3 * 5^2$

Thus $1 = \log 2 \mod 130$.

$8 \equiv 3\log 5$

$12 \equiv \log 5 + \log 7$

$14 \equiv 2\log 3(130) \Rightarrow 7 = \log 3 \mod 65$

$34 = \log_3 + 2\log 5 \mod 130$

Thus: $\log 5 \equiv 46, \log 7 \equiv 96, \log 3 \equiv 72 \mod 130$

$$\begin{bmatrix} 0 & 3 & 0 & 8 \\ 0 & 1 & 1 & 12 \\ 2 & 0 & 0 & 14 \\ 1 & 2 & 0 & 34 \end{bmatrix} \mod 130$$

$2\log 3 \equiv 14(\mod 130) \Rightarrow \log 3 \equiv 7 \mod \frac{130}{GCD(130,2)}$. Therefore $\log 3 \equiv 7 \mod 65$ so $\log 3 \equiv 7$ or $\log 3 \equiv 7 + 65 \mod 130$

Try factoring $37 * 2^r$ over $\{2, 3, 5, 7\}$ mod 130.

Turns out, $37 * 2^{43} \equiv 3 * 5 * 7 \mod 131$

$\log 37 + 43 \equiv \log 3 + \log 5 + \log 7 \mod 130$

Therefore $\log 37 \equiv 72 + 46 + 96 - 43 \mod 130 \equiv 41 \mod 130$.

Sure enough, $2^{41} \equiv 37 \mod 131$.

March 25th

Elliptic Curves - the set of all solutions (x, y) to the equation $y^2 = x^3 + ax + b$, where $x^3 + ax + b$ has no multiple (repeated) roots.

Fact: $x^3 + ax + b$ has no multiple roots if and only if $\Delta \equiv -4a^3 - 27b^2 \neq 0$

Suppose $f(x) = (x - r)g(x)$, using the product rule, $f'(x) = g(x) + (x - r)g'(x)$. Therefore r is a root of $f'(x)$ if and only if r is a root of $g(x)$. Thus $f(x) = (x - r)^2 * h(x)$.

In how many points does a line $(y = mx + k)$intersect $y^2 = x^3 + ax + b$? 3

$\{x = r\}$ meets $\{y^2 = x^3 + ax + b\}$ in two points: $x = r, y^2 = r^2 + ar + b$

Let l be the line $y = mx+k$. How many points of intersection are there between l and the elliptic curve?

Substitution of $y = mx + k$ yeilds $m^2x^2 + 2mkx + k^2 = x^3 + ax + b$. This becomes $x^3 - m^2x^2 + (a - 2mk)x + b - k^2 = 0$

Let $a = (x_1, y_1)$ and $b = (x_2, y_2)$ be on the intersection of the curve.

1. $y_1 = mx_1 + k, y_2 = mx_2 + k \Rightarrow m = \frac{y_2 - y_1}{x_2 - x_1}$ (slope)

Using the factor theorem, we have that if r_1, r_2, r_3 are the roots of $x^3 - m^2x^2 + (a - 2mk)x + b - k^2 = 0$, then $x^3 - m^2x^2 + ... = (x - r_1)(x - r_2)(x - r_3) = (x - x_1)(x - x_2)(x - r_3) \Rightarrow x^3 - m^2x^2 + ... = x^3 + x^2(-x_1 - x_2 - r_3) + ...$

Thus $-m^2 = -x_1 - x_2 - r_3$. Therefore if (x_1, y_1) and (x_2, y_2) are on the line $y = mx + k$ intersected with $y^2 = x^3 + ax + b$, the third intersection (r_3) satisfies $m^2 = x_1 + x_2 + r_3$, that is $r_3 = m^2 - x_1 - x_2$ (which gives us the x coordinate).

An example: The curve is $y^2 = x^3 - 2x + 5$. $a = (1, 2), b = (2, -3)$. The slope is therefore $m = -5$. The third root is therefore $r_3 = m^2 - x_1 - x_2 = 22$. For (r_3, s_3) is on the curve, then s_3 satisfies $s_3^2 = 22^3 - 2 * 22 + 5 = 10648 - 44 + 5 = 10609 = (\pm 103)^2$. Therefore $s_3 = 103$ or -103. Thus $(r_3, s_3) = (22, -103)$.

Def. Given $A(x_1, y_1)$ and $B(x_2, y_2)$ on the curve, let $R(r_3, x_3)$ be the third point of intersection and define $x_3 = r_3, y_3 = -s_3$, then $A + B := (x_3, y_3)$.

March 29th

Discrete Log Problem

Def. Let $p > 2$ be a prime and get GCD(n,p) = 1. Then $(\frac{n}{p}) = 1$ if $x^2 \equiv n \mod p$ has a solution and if -1 if $x^2 \equiv n \mod p$ has no solution. Also, if $p|n$, set $(\frac{n}{p}) = 0$

April 1st

Diffie-Helman Key Agreement

Public information: a large prime p, a generator (primitive element) γ of $\mathbb{Z}_p^*$

Private information:

Alice: a random integer $a \in \{2, ..., p - 2\}$

Bob: a random integer $b \in \{2, ..., p - 2\}$

Alice computes $A \equiv \gamma^a \mod p$ offline and Bob computes $B \equiv \gamma^b \mod p$ offline.

Alice sends A to Bob who sends B to Alice.

Alice computes $B^a \mod p$ and Bob computes $A^b \mod p$

Since $B^a \equiv (\gamma^b)^a \equiv \gamma^{ba} \equiv \gamma^{ab} \equiv (\gamma^a)^b \equiv A^b \mod p$

Thus B^a is the shared secret

Ex. $p = 27001, \gamma = 101$. Alice picks $a = 21768$, computes $A = \gamma^a \equiv 7580 \mod p$. Bob picks $b = 9898$, computes $B = \gamma^b \equiv 22181 \mod p$

Alice computes $B^a \equiv 10141 \mod p$. Bob does the same thing and reaches the same number. Thus the secret key $S = 10141$.

An attack on the D-H: Eve in the middle

Eve knows p and γ. Eve picks some random $z \in \{2, ..., p - 2\}$ and intercepts γ^a and γ^b. She then computes γ^z and sends it to both of them. Eve then computes $(\gamma^a)^z$ and Alice computes $(\gamma^z)^a$ thinking its $(\gamma^b)^a$. Same thing with Bob.

Thus $(\gamma^a)^z = (\gamma^z)^a = S_a, (\gamma^b)^z = (\gamma^z)^b = S_b$

Alice $\leftarrow S_a \rightarrow$ Eve $\leftarrow S_b \rightarrow$ Bob

Elliptic Curve DH

Public Info: a large prime p and a different prime q, an elliptic curve E over $\mathbb{Z}_p$ such that $|E(\mathbb{Z}_p)| = q$, and a point $p \in E$ of order q.

Private Info: Alice chooses a random $a \in \{2, ..., p-2\}$ and computes the point $A = a * p$ on E and sends A to Bob. Bob picks $b \in \{2, ..., p-2\}$ and sends $B = b * p$ to Alice.

Alice: $a * B = a * (b * p) = a * b * p = b * a * p = b * (a * p) = b * A$

April 3rd

Digital Signatures

Desired properties: uniquely identifiable, verifiable, unforgeable, tied to document, timestamp, sender cannot repudiate

RSA signature scheme

Setup: $n = pq$ where p,q prime, e and d encryption and decryption exponent.

Alice sends message (m) to Bob.

Alice establishes her RSA system with n_A, her public mod and e_A, d_A, her encryption and decryption exponents.

Alice sends $y \equiv m^{d_A} \mod n_A$ (the signature) and m (the message)

The signature is (m, y).

Bob computes $s \equiv y^{e_A} \mod n_A$.

$s \equiv m \mod n_A$, verification is ok. $s \not\equiv m \mod n_A$, verification is not ok.

Note: say $s \equiv y^{e_A} \equiv (m^{d_A})^{e_A} \equiv m^{d_A e_A} \equiv m \mod n_A$. $d_A e_A \equiv 1 \mod n_A, \phi(n)|de \Rightarrow m^{de} \equiv m \mod n$

El Gamal:

Public parameters: large prime p, primitive element $\alpha \in \mathbb{Z}_{|}^*$, $\beta \equiv \alpha^a \mod p$

Private parameters: an exponent $a \in \{2, ..., p-2\}$

Alice sends a pair (y_1, y_2) to Bob.

Alice picks $k \in \{2, ..., p-2\}$, sends $y_1 \equiv \alpha^k \mod p$ and $y_2 \equiv m * \beta^k \mod p$

GCD$(k, p-1) = 1$ (relatively prime)

Bob computes $y_2(y_1^{-1})^a \mod p \equiv m * \beta^k * (\alpha^k)^{-a} \equiv m(\alpha^{ak} * \alpha^{-ak}) \mod p \equiv m \mod p$

El Gamal is slow and complicated!

El Gamal signature scheme:

Alice computes $\gamma \equiv \alpha^k \mod p$ $(\gamma = y_1)$ and $\delta \equiv (m - a\gamma) * k^{-1} \mod p-1$.

For a signature scheme, GCD$(k, p-1) = 1$.

Alice sends (m, γ, δ) to Bob.

Bob computes $v_1 \equiv \beta^\gamma * \gamma^\delta \mod p$ and $v_2 \equiv \alpha^m \mod p$.

Verification is ok if and only if $v_1 \equiv v_2 \mod p$

Want $\alpha^m \equiv \beta^\gamma \gamma^\delta \mod p$. Leave γ as in the exponent. Therefore $\alpha^m \equiv \alpha^{a\gamma}\gamma^\delta \mod p \equiv \alpha^{a\gamma}\alpha^{k*\delta} \mod p \equiv \alpha^{a\gamma + k\delta} \mod p$ thus α primitive where the previous holds if and only if $m \equiv a\gamma + k\delta \mod p-1$.

April 5th

ElGamal in $\mathbb{Z}_p^*$, p a large prime

a is for long-term use, k is short-term (session key)

Example. $p = 467, \alpha = 2, a = 127, \beta = 2^{127} \equiv 132 \mod p$

Alice signs $m = 100$, using $k = 213$

Then $k^{-1} \equiv 431 \mod p$

Alice calculates $\gamma = 2^{213} \equiv 29 \mod p$ and $\delta = (100 - 127 * 29)431 \mod p - 1 \equiv 51$

Thus signature is (100,29,51)

$v_2 = 2^{100} \equiv 189 \mod p$ and $v_1 = 132^{29} * 29^{51} \mod p \equiv 189 \mod p$

Hash function: a mapping $h : S \to T$ where S is a set of strings of arbitrary length and T the set of all strings of some fixed length

for DSA (digital signature algorithm), $T = 160$ bit strings

Public parameters: p is an L-bit prime, $512 \leq L \leq 1024$, q is a 160-bit prime such that $q|p-1$, g is a primitive element mod p ($\text{ord}_p(g) = p-1$), h is a hashing function mapping arbitrary strings into 160-bit strings, $\alpha \equiv g^{\frac{p-1}{2}} \mod p$

Note g has order $p-1$ so $\alpha \equiv g^{\frac{p-1}{2}} \mod p$ has order $q - \alpha^q \equiv 1 \mod p$. where $\beta \equiv \alpha^a \mod p$ (a is Alice's private info)

To sign m, Alice picks $k \in \{2, ..., q-2\}$

Alice computes $\gamma \equiv (\gamma^k \mod p) \mod q$. $\delta \equiv (h(m) + a(\gamma))k^{-1} \mod q$

Alice sends (m, γ, δ)

a is a long-term private key, k is a short message key

Bob computes $e_1 \equiv h(m)\delta^{-1} \mod q$ and $e_2 \equiv \gamma\delta^{-1} \mod q$

Verification is ok if and only if $(\alpha^{e_1}\beta^{e_2} \mod p) \mod q = \gamma$

April 8th

Secret splitting - dealer wants to split a secret value M between A and B

D picks a random positive integer, gives r to Alice, M-r to Bob.

Pick n > any potential msg. D picks a random integer r mod n. Gives r to Alice (r mod n) and M-r to Bob (M-r mod n)

Add C to this, give r to A, s to B, M-(r+s) to C

Def. Let $0 < t \leq w$, positive integers

A (t, w) threshold scheme is a way to share a message value M among w participants such that

1. any t or more participants can reconstruct the message
2. but no set of $\leq t-1$ participants can do so

Let p be a prime $\geq w+1$. Dealer constructs a polynomial $f(x)$ with coefficients in $\mathbb{Z}_p$ of degree $\leq t-1$. say $f(x) = a_0 + a_1x + ... + a_{t-1}x^{t-1}$.

The dealer assigns player i the share (x_i, y_i) where $y_1 \equiv f(x_1) \mod p$. The secret is a_0.

Ex. $p = 17, t = 3, w = 5$, P_1, P_3, P_5 are collaborating.

$P_1 = (1, 8), P_3 = (3, 10), P_5 = (5, 11) \mod 17$.

(1) $a_0 + a_1 + a_2 \equiv 8 \mod 17$

(3) $a_0 + 3a_1 + 9a_2 \equiv 10 \mod 17$

(5) $a_0 + 5a_1 + 25a_2 \equiv 11 \mod 17$

Solve the system to get $a_1 \equiv 10, a_2 \equiv 2, a_0 \equiv 13 \mod 17$

The polynomial $f(x)$ has a very nice expression as a sum of t terms, each term being almost a poly $l_j(x)$ with the feature that $l_j(x_R) = 0$ if $j \neq k = 1$ if $j = k$. Thus $f(x) = l_1(x)y_1 + l_2(x)y_2 + ... + l_t(x)y_t$

April 10th

Threshold schemes

From a population of w participants, devise a scheme such that any t or more participants can determine the value, but any fewer than t participants cannot.

A polynomial $f(x)$ of degree $t-1$ can be determined uniquely given any t distinct points.

P_i gets (x_i, y_i) we have $y_i = f(x_i) = a_0 + a_ix_i + ... + a_{t-1}x_i^{t-1}$ with $a_1, ..., a_{t-1}$ are randomly chosen from $[1..q]$ where q is a prime "large enough" and arithmetic in mod q and a_0 is the secret.

Let $V = \begin{bmatrix} 1 & x_1 & x_1^2 & ... & x_1^{t-1} \\ 1 & x_2 & x_2^2 & ... & x_2^{t-1} \\ . & ... & ... & ... & ... \\ 1 & x_t & x_t^2 & ... & x_t^{t-1} \end{bmatrix}$

$det(V) = \sum_{i<j}(x_j - x_i) \not\equiv 0 \mod q$ because x_is are all different.

Therefore can solve for $a_i : V \begin{bmatrix} a_0 \\ ... \\ a_{t-1} \end{bmatrix} = \begin{bmatrix} y_1 \\ ... \\ y_t \end{bmatrix}$

(1) Find polynomials $l_i(x)$ where $1 \leq i \leq t$ such that $l_i(x_j)$ is 1 if $i = j$ and 0 if $i \neq j$

Ex. t = 4, i = 3.

$g(x) = (x-x_1)(x-x_2)(x-x_4)$: $g(x_j) = 0$ if $x_j = x_1, x_2, x_4$. $g(x_3) = (x_3 - x_1)(x_3 - x_2)(x_3 - x_4) \neq 0$.

Let $l_3(x) = \frac{(x-x_1)(x-x_2)(x-x_4)}{(x_3-x_1)(x_3-x_2)(x_3-x_4)}$.

$(x_1, y_1), ..., (x_4, y_4)$ given points on curve.

$L(x) = y_1l_1(x) + y_2l_2(x) + y_3l_3(x) + y_4l_4(x) = a_0 + a_1x + a_2x^2 + a_3x^3$

$L(0) = a_0$ is the secret.

$L(x) = \sum_{i=1}^{t} y_il_i(x)$

Therefore $L(0) = q = \sum_{l=i}^{t} y_il_i(0)$

$l_i(x) = \prod_{j \neq i} \frac{x-x_j}{x_i-x_j}$. Therefore $l_i(0) = \prod_{j \neq i, 1 \leq j \leq t} \frac{-x_j}{(x_i - x_j)}$

Therefore $L(0) = a_0 = \sum_{i=1}^{t} y_i \prod_{j \neq i} \frac{-x_j}{x_i-x_j}$

$(4, 25), (-7-85), (2, 19)$. $L(0) = a_0 = \sum_{i=1}^{t} y_i \prod_{j \neq i} \frac{-x_j}{x_i-x_j} = \sum_{i=1}^{3} y_i \prod_{j \neq i} \frac{-x_j}{x_i-x_j} = y_1(\frac{7}{4+7})(\frac{-2}{4-2}) + y_2(\frac{-4}{-7-4})(\frac{-2}{-9}) + y_3(\frac{-4}{2-4})(\frac{7}{2+7}) = 25(\frac{7}{11})(\frac{-2}{2}) - 85(\frac{-4}{-11})(\frac{-2}{-9}) + 19(\frac{-4}{-2})(\frac{7}{9}) = \frac{61}{9}$???

April 15th

Variations on Shamir's Scheme

A scheme with t = 8

Boss has 4 shares, daughter have 2 shares apiece. workers have one share apiece.

daughters $n_d \geq 4$ or # workers $n_w \geq 8$

A scheme with two companies A and B

They agree that it takes 4 members of company A and three members of B to secure the key (Secret)

Company A has a secret S_A and B has another secret S_B. Secret S_A is obtained using a threshold scheme with t = 4 and S_B is obtained using t = 3.

Master secret = $S_A + S_B$

A military organization has a general, two colonals, and five recruits.

Only three combinations are allowed:

The general, both colonels, all 5 grunts, or one colonel and 3 grunts.

etc..

Blakley's Threshold Scheme

For shamir used $l_i = \prod\limits_{j \neq i} \frac{(x-x_j)}{x_i - x_j}, L(x) = \sum\limits_{i=1}^{t} y_i * l_i(x)$, secret is $L(0)$

$t = 3$, let x_0 = secret. Let p be a large prime

Pick $y_0, z_0 \in$ Random(p)

Let $Q = (x_0, y_0, z_0)$ in 3D mod p

For each player, assign $a_i, b_i \in$ Random(p), $1 \leq i \leq t$

Set $c_i = z_0 - a_i x_0 - b_i y_0 \mod p$

Note that $z \equiv a_i x + b_i y + c_i \mod p$ is a "plane" in 3D over $\mathbb{Z}_p$

April 22nd

Zero knowledge proofs

Results: Let p be an odd prime, and let g be a primitive element mod p (ie. $F_p^* = \{g, g^2, ..., g^{p-1}\}$)

There exists exactly $\frac{p-2}{2}$ square mod p, a is a square mod p means $X^2 \equiv a \mod p$ has a solution and $p \not| a$.

If $1 \leq i, j \leq \frac{p-1}{2}$, then $i^2 \equiv j^2 \mod p$ means $p | (i-j) * (i+j)$. Primality $\Rightarrow p | i - j$ or $p | i + j$. If $i \neq j$, then $p | i + j$. But $2 \leq i + j \leq p - 1$. Therefore $p \not| i + j$. So there exists at least $\frac{p-1}{2}$ squares mod p.

The squares mod p are exactly the even powers $g^2, g^4, ..., g^{p-1}$ mod p. The nonsquares are the odd powers of g mod p.

If a is a square mod p, then $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

If a is a nonsquare mod p, then $a^{\frac{p-1}{2}} \equiv -1 \mod p$.

Proof. First, g is a generator (primitive element) mod p so its order is $p-1$, which means $g^{p-1} \equiv 1 \mod p$ and $g^{\frac{p-1}{2}} \not\equiv 1 \mod p$.

$(g^{\frac{p-1}{2}})^2 \equiv 1 \mod p$ so $g^{\frac{p-1}{2}} \equiv -1 \mod p$ where p is a prime.

Suppose a is a square

Ex. $p = 19, g = 2$ is a primitive element.

Suppose a is a square mod p. Then $a \equiv g^{2k} \mod p$, so that $a^{\frac{p-1}{2}} \equiv (g^{2k})^{\frac{p-1}{2}} \equiv (g^{p-1})^k \equiv 1 \mod p$.

Suppose a is a nonsquare mod p. Then $a \equiv g^{2l+1} \mod p$ and so $a^{\frac{p-1}{2}} = g^{(2l-1)(\frac{p-1}{2})} \equiv (g^{p-1})^l * g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \mod p$.

Euler's Criteron: If p is an odd prime and $(a,p) = 1$, then $a^{\frac{p-1}{2}} \equiv 1$ or -1 mod p, according as a is or is not a square mod p.

Key Lemma: Let $p \equiv 3 \mod 4$. If a is a square mod p, define $b := a^{\frac{p+1}{4}} \mod p$. Then $b^2 \equiv a \mod p$.

Ex. 7 is a square: $a = 7, p = 19$, so $\frac{p+1}{4} = 5$. $b = 7^5 * b^2 = y^{10}$, $b = 11$, $b^2 = 121 = 7 + b * 19$.

Proof: $b^2 \equiv (a^{\frac{p+1}{4}})^2 \mod p \equiv a^{\frac{p+1}{2}} \mod p \equiv a^{\frac{p-1+2}{2}} \mod p \equiv a^{\frac{p-1}{2}} * a \mod p \equiv 1 * a \equiv a \mod p$ as claimed.

Ex. (a zero knowledge proof) Bob finds two large primes p and q such that $p \equiv q \equiv 3 \mod 4$, and construct $n = pq$.

Bob tells Alice "I know the factorization of n."

Alice chooses x at random between 1 and n, sends Bob the number y where y is the least positive residue of $x^4 \mod n$.

(challenge - response - notification)

Bob receives y from Alice, knows y is a square mod n. Since $y \equiv x^4 \equiv (x^2)^2 \mod n$, it is also true that $y \equiv (x^2)^2 \mod p$ and $q \equiv (x^2)^2 \mod q$.

Bob computes $\pm y^{\frac{p+1}{4}} \mod p$ and $\pm y^{\frac{q+1}{4}} \mod q$. These give 4 square roots of y mod pq by the Chinese Remainder Theorem.

However, only one of these square roots of y is itself a square!

Bob finds the value $v \mod n$ that is in fact a perfect square and sends it to Alice.

Alice knows x, and so computes $x^2 \mod n$. If $x^2 \equiv v \mod n$, verification is achieved.

April 24th

Alice knows only n, Bob knows $n = pq$, $p \equiv q \equiv 3 \mod 4$

Alice picks $x \in$Rand(n), sends $y \equiv x^4 \mod n$ to Bob.

Bob receives y from Alice, computes $a = \pm y^{\frac{p+1}{4}} \mod p$. Saw that $y^{\frac{p+1}{4}}$ is a sqrt of y mod p if y is a square. $b = \pm y^{\frac{q+1}{4}} \mod q$.

Exactly one of hte four systems $w \equiv \pm a \mod p$, $w \equiv \pm b \mod q$ has a solution that is a perfect square mod pp and mod q and therefore mod n.

Bob sends w to Alice.

Alice computes $x^2 \mod n$. If $x^2 \equiv w \mod n$, then verification is Ok.

Shamir's zero knowledge proof protocol (Repeatable protocol)

Bob chooses $p \equiv q \equiv 3 \mod 4$, sends $n = pq$ to Alice.

Picks some integer I that represents some sort of personal ID

Finds a small positive integer c such that $v = I||c$ is a square mod both p and q (and thus n)

Note: Bob can find a square root v mod p and mod q and hence mod n. There exists u such that $v \equiv u^2$ mod n

Bob sends v to Alice.

1. Bob chooses $r \in$Random[n], sends Alice two values: $x \equiv r^2 \mod n$ and $y \equiv vx^{-1} \mod n$

2. Alice checks that the product $xy \equiv v \mod n$. Alice has seen $v = I||c \mod n$ and x and y.

Alice then picks a random bit $b = 0$ or 1, sends to Bob.

3. If $b = 0$, Bob sends r to Alice. If $b = 1$, Bob sends ur^{-1} to Alice

4. Alice squares what she receives mod n.

If $b = 0$, Alice squares r, sees $r^2 \equiv x \mod n$

If $b = 1$, Alice squares $(ur^{-1})^2 \equiv vr^{-2} \equiv vr^{-1} \equiv y \mod n$

If $b = 0$ and answer $= x$ or if $b = 1$ and answer $= y$, verification is achieved.

Finding squares

Let p be an odd prime and let GCD$(a, p) = 1$.

Define the Legendre Symbol $(\frac{a}{p})$ by $(\frac{a}{p}) = 1$ if $x^2 = a \mod p$ has a solution and $= -1$ if there is no solution. Thus $(\frac{7}{19}) = 1$ because $7 \equiv 64 \equiv 8^2 \mod 19$.

$(\frac{a}{p})$ satisfies some rules:

1. Let GCD$(a, p) =$ GCD$(b, p) = 1$, then $(\frac{a^2}{p}) = 1$
2. If $a \equiv b \mod p$, then $(\frac{a}{p}) = (\frac{b}{p})$
3. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$
4. Euler's criteron: $\frac{p-1}{2}, (\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \mod p$
5. The special cases:
   (a) $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = 1$ if $p \equiv 1 \mod 4$ and -1 if $p \equiv 3 \mod 4$
   (b) $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = 1$ if $p \equiv \pm 1 \mod 8$ and -1 if $p \equiv \pm 3 \mod 8$
   (c) If p and q are distinct odd primes, then $(\frac{p}{q}) = (\frac{q}{p})(-1)$

April 29th

S-T

Given p a prime, with GCD$(a, p) = 1$, Find $x : x^2 \equiv a \mod p$ or show none exists

Compute $(\frac{a}{p})$. If it is -1, stop., else go

Write $p - 1 = 2^s t$, t odd. Find $n : (\frac{n}{p}) = -1$

Initialize $x = a^{\frac{t+1}{2}}$ (initial guess), $b = a^t$ (correction factor), $g = n^t$ and $\text{ord}_p g = 2^s = g^{2^{s-1}} = n^{t*2^{s-1}} = n^{\frac{p-1}{2}} \equiv (\frac{n}{p}) \equiv -1 \mod p$

flag $= 1$, $r = s$, while flag != 0, find least m where $0 \leq m \leq r - 1$ with $b^{2^m} \equiv 1 \mod p$

if m = 1, break and return x. else update $x = x_{next} = x * g^{2^{r-m-1}}, b = b_{next} = b * g^{2^{r-m}}, g = g_{next} = g^{2^{r-m}}, r = r_{next} = m$

Example: $p = 113$

$(\frac{2}{p}) = 1, p - 1 = 167 = 2^4 7, s = 4, t - 7.$