Modern Ciphers

CMPUT 396

Public-Key Cryptography

- Key distribution has always been a serious problem for military and business cryptography.
- In 1975, Diffie proposed an asymmetric key cipher.
- The idea was to create a strong cipher that does not obey the "last on, first off" principle.
- The "double padlock" metaphor: both the sender and the recipient apply their own locks.
- Modular arithmetic yields an encryption function that is easy to do but difficult to undo.

DHM Key Exchange

- DHM is a method of exchanging keys over a public channel.
- DHM is based on the idea of **one-way function**.
- Alice and Bob publicly agree on a **modulus** p and **base** g.
- Alice and Bob choose their own secret integers a and b.
- Alice sends g^a mod p to Bob; Bob sends g^b mod p.
- Alice and Bob now share a secure secret key.
- The key is: $(g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$

DHM Example

- g = 5 (public prime base)
- p = 23 (public prime modulus)
- a = 6 (Alice's private number)
- b = 15 (Bob's private number)
- $A = g^a \bmod p = 8$ (Alice's public number)
- $B = g^b \bmod p = 19$ (Bob's public number)
- $s = B^a \bmod p = A^b \bmod p = 2$ (the shared key)

Prime Numbers

- A *prime* number has only two factors: 1 and itself.
- Every integer except 1 is either *prime* or *composite*.
- There are infinitely many primes.
- Algorithms to check if a number is prime:
  - Sieve of Erathoshenes (200 BC, table)
  - Trial division (1200 AD, simple but slow)
  - Rabin-Miller (1967, fast, but not perfect)
  - AKS (2002, polynomial but slow)

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Fermat's Little Theorem

- *If p is a prime, then for any a, $a^p - a$ is a multiple of p*:

  $a^p \bmod p = a$, (i.e. $a^{p-1} \bmod p = 1$)

- E.g. a = 2, p = 7: $2^7 = 128 = 7 \times 18 + 2$
- This theorem is used for Fermat's primality test:
  - we want to find out if *p* is prime
  - pick a random *a* in the range $[2, p-1]$
  - Does $a^p \bmod p = a$ hold?
    - if it doesn't, then *p* is composite (i.e. *not* prime)
    - if it does, then *p* is *probably* prime
- This is a special case of the Euler's totient theorem:

  $a^{(p-1)(q-1)} \bmod (pq) = 1$

RSA Cryptosystem

- Alice creates a public key:
  - picks large secret *primes* p and q
  - computes n = pq
  - picks random e in [2, n−1], *coprime* to (p−1)(q−1)
  - finds *modular inverse* $d = e^{-1} \bmod (p-1)(q-1)$
  - publishes n and e, but keeps secret p, q, and d
- Bob sends encrypted message to Alice:
  - converts the text to a number M
  - computes $C = M^e \bmod n$, and sends C to Alice
- Alice decrypts message from Bob
  - computes $M = C^d \bmod n$

Public and Private Keys

- RSA Example:
  - p = 11, q =13, n = 143, (p−1)(q−1) = 120
  - e = 23, coprime to 120
  - d = 47, modular inverse of 23 mod 120
  - public key: (n=143, e=23)
  - private key: (n=143, d=47)
  - $M = 84$; $C = 84^{23} \bmod 143 = 24$; $M = 24^{47} \bmod 143 = 84$
- RSA Correctness:
  - $d = e^{-1} \bmod (p-1)(q-1) \rightarrow e*d = k(p-1)(q-1) + 1$ (Fermat)
  - $M = C^d \bmod n$ *and* $C = M^e \bmod n$
  - $M = C^d = (M^e)^d = M^{e*d} = M^{(p-1)(p-1)k+1} = (1)^k M^1 = M$

RSA Block Encoding

- A text message is converted into a list of blocks.
- A block is a large integer that encodes a fixed-length string of characters.
- The maximum block size depends on the symbol set size S and key size:

$$S^{|block|} \leq 2^{|key|}$$

- e.g., |key| = 1024, S = 66 → |block| ≤ 169
- encoding: block = $\Sigma_i \text{index}(c_i) * S^i$
- e.g., index('R')* 66^0 + index('S')* 66^1 + index('A') * 66^2

RSA Security

- Brute-force? *Too many keys.*
- Dictionary attack? *Keys are numbers, not words.*
- Word pattern attack? *Letter encoding is not fixed.*
- Frequency analysis? *Each block encodes a string.*
- Compute M from C? *Discrete logarithm problem.*
- Compute p and q? *Integer factorization problem.*
- See Wikipedia on how to crack a naive implementation of RSA.

Pretty Good Privacy

- before the Information Age cryptography was the exclusive domain of governments and military
- RSA was designed for business applications
- dark side: organized crime and terrorists
- governments can easily intercept all e-mails
- right to privacy: make RSA available to everyone
- PGP features (1991):
  - symmetric secret-key cryptosystem
  - key and signature exchanged with RSA
  - random public/private key generation
- Zimmerman investigated as an arms dealer

Teacher's Question

Do you think that monitoring electronic communications to prevent terrorist attacks and organized crime is justified even if it infringes on everyone's right to privacy?