RSA

Need large prime #'s

prime numbers are fairly frequent
even for 100+ digit numbers.

Need to be able compute $\phi(n)$
where $n = p \cdot q$ $\quad \phi(p \cdot q) = (p-1)(q-1)$

Need to pick a big number d
such that $\gcd(d, \phi(n)) = 1$
and compute $e \equiv d^{-1} \pmod{\phi(n)}$

publish e, n

keep secret d, $\phi(n)$

However if I can compute p & q from
n then d & $\phi(n)$ are no longer
secret.

Variations of DES

- **triple-DES**: In effect, the input is encrypted three times. One such method uses the keys k_1, k_2, and k_3 to define

$$C = E_{k_3}(D_{k_2}(E_{k_1}(M)))$$

where E_k and D_k represent DES encryption and DES decryption, respectively.

- **DESX**: plaintext is bitwise XORed with 64 bits of additional key material before encryption with DES and the output is also bitwise XORed with another 64 bits of key material.

Merkle-Hellman Knapsack Cryptosystem

1. Choose a superincreasing sequence

$$s_1, s_2, \ldots, s_n. \leftarrow \text{secret}$$

2. Choose p to be a large prime such that

secret

$$p > s_1 + s_2 + \cdots + s_n.$$

3. Let a be a random number between 1 and $p-1$ and publicly announce

public $\longrightarrow t_i := as_i \mod p.$

Encryption Process: To encode a message $(x_1, x_2, \ldots, x_n)$ (made of bits of 0 and 1), one sends the single number

$$C := \sum_{i=1}^{n} x_i t_i. \quad (\text{mod } p)$$

Encryption Process: To decode, we need only solve the subset sum problem for

$$\begin{aligned} M &:= a^{-1} C \mod p. \\ &= a^{-1} \sum_{i=1}^{n} x_i a s_i \qquad (\text{mod } p) \\ &= \sum_{i=1}^{n} x_i s_i \end{aligned}$$

super increasing sequence

$5, 17, 30, 59, 130, 281 \leftarrow s_i$

$219 = 130 + 89 = 130 + 59 + 30$

$222 = 130 + 92 = 130 + 59 + 33$

Subset Sum Problem

Given a positive integer T and the following sequence of positive integers

$$s_1, s_2, \ldots, s_n,$$

find a sequence $1 \leq i_1 < i_2 < \ldots < i_k \leq n$ such that

$$T = s_{i_1} + s_{i_2} + \ldots + s_{i_k}.$$

Example:

$$\{14, 28, 56, 82, 90, 132, 197, 284, 341\}$$

$$\begin{aligned} 515 &= 341 + 132 + 28 + 14 \\ &= 341 + 90 + 56 + 28 \\ &= 197 + 132 + 90 + 82 + 14 \end{aligned}$$

On the otherhand, there are no subset sums for 516.

This problem has been shown to be "**NP-complete**", which means that (among other things) there is no known polynomial-time algorithm that solves it.

Analysis of Quadratic Sieve

Claim: If $m = pq$ where $p, q > 1$, then for all $a \in \{1, 2, \ldots, (m-1)/2\}$ such that $gcd(a, m) = 1$, there is an integer $b \in \{1, 2, \ldots, (m-1)/2\}$ such that $b \neq a$ and $b^2 \equiv a^2 \bmod m$.

$1^2 \equiv 8^2 \pmod{21}$

$2^2 \equiv 5^2 \pmod{21}$

$4^2 \equiv 10^2 \pmod{21}$

Example: $m = 21$

a	$gcd(a, m)$	$a^2 \bmod m$	b
1	1	1	8
2	1	4	5
~~3~~	~~3~~	~~9~~	
4	1	16	10
5	1	4	2
~~6~~	~~3~~	~~15~~	
~~7~~	~~7~~	~~7~~	
8	1	1	1
~~9~~	~~3~~	~~18~~	
10	1	16	4

Data Encryption Standard (DES)

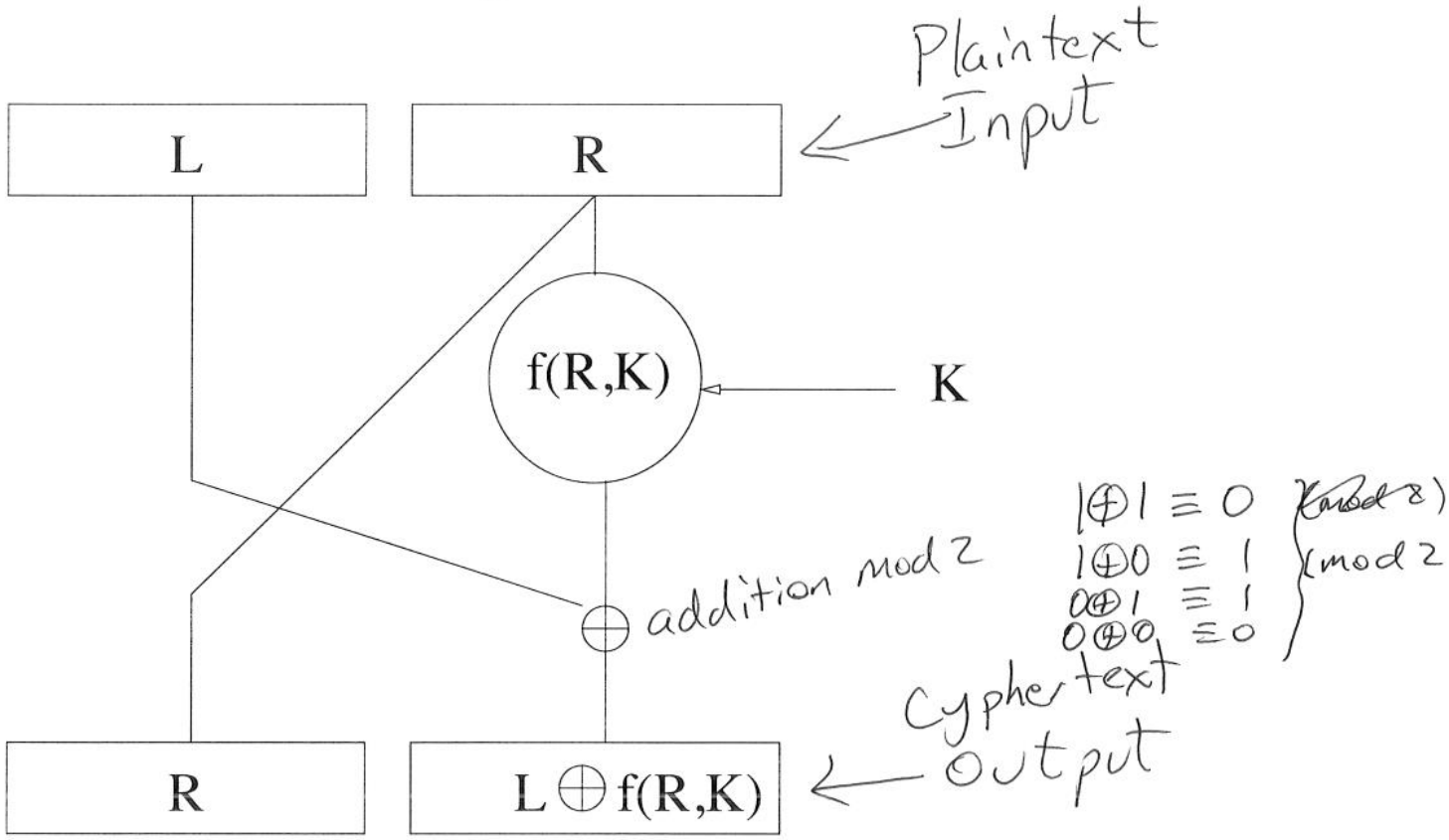
classical cryptography

security relies on secrecy of keys

- Originally developed under the name Lucifer by IBM in the 60's and 70's
- Adopted by Federal government in July, 1977
- Reaffirmed in 1983, 1988, 1993, and 1999
- Most widely used cryptosystem in the world from 1977 to present
- Used by the U.S. Government to "protect the confidentiality of sensitive (unclassified) electronic information".
- Replaced by AES (Rijndael) in Summer of 2001

Note in modern cryptography secrecy depends on computation of keys is difficult to do.

Feistel Cipher



$1 \oplus 1 \equiv 0$
$1 \oplus 0 \equiv 1$
$0 \oplus 1 \equiv 1$
$0 \oplus 0 \equiv 0$
(mod 2

Selection Function S_1

0000 0
0001 1
0010 2
0011 3
0100 4
0101 5
0110 6
0111 7
1000 8
1001 9
⋮

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

00 = 0
01 = 1
10 = 2
11 = 3

Example: 110100

- Use first and last digit as row index: 10 (base 2) = 2
- Use middle four digits as column index: 1010 (base 2) = 10
- The number 9 appears in row 2, column 10
- 9 = 1001 (base 2)

$$S_1(110100) = 1001$$