Exercise 1 – Perfect Secrecy

- Let us consider the following cryptosystem
- P = {a, b, c};
- Pr(a) = 1/2; Pr(b) = 1/3; Pr(c) = 1/6
- K = {k1, k2, k3};
- Pr(k1) = Pr(k2) = Pr(k2) = 1/3;
- C = {1, 2, 3, 4};

P=Plaintext
C=Ciphertext
K=Key

Encryption Matrix

	a	b	c
k1	1	2	3
k2	2	3	4
k3	3	4	1

Exercise 1 – Perfect Secrecy

- Compute the probability distribution of the **ciphertext**
- Compute the *Conditional probability* distribution on the **Plaintext**, given that a certain ciphertext has been observed (using Bayes)

$$\Pr[x \mid y] = \frac{\Pr[y \mid x]\Pr[x]}{\Pr[y]}$$

DOES THIS CRYPTOSYSTEM HAVE PERFECT SECRECY?

Exercise 1 - Solution

- $P(1)=2/9$, $P(2)=5/18$, $P(3)=1/3$, $P(4)=1/6$

$P(a\|1)=3/4$	$P(b\|1)=0$	$P(c\|1)=1/4$
$P(a\|2)=3/5$	$P(b\|2)=2/5$	$P(c\|2)=0$
$P(a\|3)=1/2$	**$P(b\|3)=1/3$**	**$P(c\|3)=1/6$**
$P(a\|4)=0$	$P(b\|4)=2/3$	$P(c\|4)=1/3$

Exercise 2 – Affine Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

- Encrypt the plaintext 'howareyou' using the affine function:
  - $e(x) = 5x+7 \bmod 26$
- Find the decryption function d(y)
- Check that it works by decyphering what you obtained

In practical situations, the « invmodn » function found here can be used
http://www2.math.umd.edu/~lcw/MatlabCode/

Exercise 2 - Solution

- Changing the plaintext to numbers yields
  - 7, 14, 22, 0, 17, 4, 24, 14, 20.
- Applying 5x+7 to each yields
  - $5 \cdot 7+7 = 42 \equiv 16 \pmod{26}$, $5 \cdot 14+7 = 77 \equiv 25$ …
- Changing back to letters yields ‘QZNHOBXZD’ as the ciphertext.
- $y = 5x+7 \bmod 26$, $x=5^{-1}(y-7) \bmod 26$
  - $x=21y+9 \bmod 26$

- Note that $5*21=105=1 \bmod 26$

Exercise 3 – Key space of Affine Ciphers

- Suppose we use an affine cipher modulo 26.
- How many keys are possible ?
- What if we work modulo 27 ?
- What if we work modulo 29 ?

Exercise 3 - Solution

- For an affine cipher $mx + n \pmod{26}$, we must have $\gcd(26,m) = 1$, and we can always take $1 \le n \le 26$.
  - $\phi(26)= \phi(2*13)=(2-1)*(13-1)= 12$, hence we have $12*26=$**312** possible keys.
- For an affine cipher $mx + n \pmod{27}$, we must have $\gcd(27,m) = 1$, and we can always take $1 \le n \le 27$.
  - $\phi(27)=\phi(3^3)=3^3 -3^2 =27-9 = 18$
  - All 27 values of n are possible
  - So we have $18 \cdot 27 =$ **486** keys.
- When we work mod 29, all values $1 \le m \le 28$ are allowed, $\phi(29)=29-1=28$,
  - so we have $28 \cdot 29 =$ **812** keys.

Exercise 4 – Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

- Caesar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the *river*) or at the Coliseum (the *arena*). He sends the ciphertext ‘EVIRE’. However, Marc Antony does not know the key, so he tries all possibilities.

- Where will he meet Caesar ?

Exercise 4 - Solution

- Among the shifts of EVIRE, there are two words: “arena” and “river”. Therefore, Marc Anthony cannot determine where to meet Caesar !

Exercise 1 - RSA

- Let us consider an RSA Public Key Crypto System
- Alice selects 2 prime numbers:
  - p=5, q=11
- Compute n, and Φ(n)
- Alice selects her public exponent e = 3
- Is this choice for "e" valid here? Is this choice *always* valid ?
- Compute d , the *private* exponent of Alice

In practical situations, the « invmodn » function found here can be used
http://www2.math.umd.edu/~lcw/MatlabCode/

Exercise 2 - RSA

- Now *you* want to send message M=4 to Alice
- Encrypt your plaintext M using Alice public exponent/ What is the resulting ciphertext C?
- Now Alice receives C
- Verify that Alice can obtain M from C, using her *private* decryption exponent
  – Hint: use square and multiply

Exercise 2 - Solution

- n=pq=55
- $\Phi(n) = (p-1)(q-1)=4x10=40$
- Gcd(3,40)=1, e=3 is a valid choice (note that 3 is a prime number)
- Alice private exponent d: de=1 mod $\Phi(n)$, hence 3d=1 mod 40
- **d=27** since 3*27=81 = 1 mod 40
- You send: **C** = M^e mod n = 4^3 mod 55 = 64 mod 55 = **9**
- Alice receives C and computes C^d mod n = 9^{27}mod 55=4

Exercise 2 - Solution

- Let us compute 9^{27} mod 55
- x=9, n=55, c=27 = 11011 (binary form)

i	c_i	*z*
4	1	1^2x 9=9
3	1	9^2x 9=729 mod 55 = 14
2	0	14^2=31
1	1	31^2x 9=14
0	1	14^2x 9=**4**

Exercise 3

- Alice uses the RSA Crypto System to receive messages from Bob. She chooses
  - $p=13$, $q=23$
  - her public exponent $e=35$
- Alice published the product $n=pq=299$ and $e=35$.
- Check that $e=35$ is a valid exponent for the RSA algorithm
- Compute d , the *private* exponent of Alice
- Bob wants to send to Alice the (encrypted) plaintext $P=15$.
- What does he send to Alice ?
- Verify she can decrypt this message

Exercise 3 - Solution

- First of all, $\Phi(n) = (p-1)(q-1)=264$
- To be valid, $gcd(e, \Phi(n))$ must be = 1
  - $Gcd(35,264)=1$, indeed since $35=5*7$ and $264=2^3*3*11$
- The private exponent $d = e^{-1} \bmod \Phi(n) = 35^{-1} \bmod 264$
- d=83

  2^3
- $d = 35^{\Phi(264)-1} = 35^{\Phi(8)\,\Phi(3)\,\Phi(11)-1} = 35^{4*2*10-1} = 35^{79} \bmod 264 = 83$

i	c_i	z
6	1	1^2x 35=35
5	0	35^2=169
4	0	169^2=49
3	1	49^2x 35=83
2	1	83^2x 35=83
1	1	83^2x 35=83
0	1	83^2x 35=**83**

Exercise 3 - Solution

- So, $C=P^e \bmod n = 15^{35} \bmod 299 = 189$
- And $P= C^d \bmod n = 189^{83} \bmod 299 = 15$

Exercise 4 – Digital Signature with RSA

- Alice publishes the following data
  - $n = pq = 221$ and $e = 13$.
- Bob receives the message P = 65 and the corresponding digital signature S = 182.
- Verify the signature

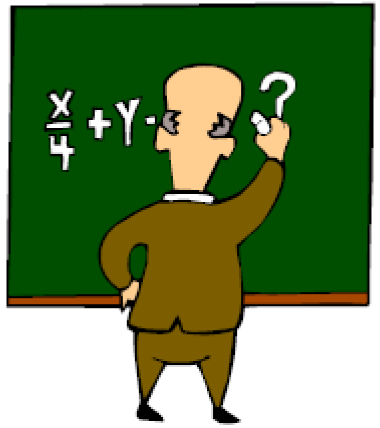
Exercise 4 – Solution

- The signature is valide if
  - $P = S^e \bmod n.$
- In our case:
  - $S^e \bmod n = 182^{13} \bmod 221 = 65,$ which is valid

Attacks against RSA

Math-Based Key Recovery Attacks

- Three possible approaches:
  1. Factor n = pq
  2. Determine Φ(n)
  3. Find the private key d directly
- All the above <u>are equivalent</u> to factoring n



Knowing Φ(n) Implies Factorization

- If a cryptanalyst can learn the value of Φ(n), then he can factor n and break the system. In other words, computing Φ(n) is no easier than factoring n
- In fact, knowing both n and Φ(n), one knows

$$n = pq$$
$$\Phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - n/p + 1$$
$$p\Phi(n) = np - p^2 - n + p$$
$$p^2 - np + \Phi(n)p - p + n = 0$$
$$p^2 - (n - \Phi(n) + 1)\, p + n = 0$$

- There are two solutions of p in the above equation.
- Both p and q are solutions.

Exercise 1 - Factorization

- Alice set us an RSA cryptosystem.
- Unfortunately, the cryptalyst has learned that $n = 493$ and $\Phi(n) = 448$.
- Find out the two factors of n.
- Supposing the public exponent of Alice is $e=3$, find her private exponent d.

Exercise 1 - Solution

- Find out the two factors of n.
- $p^2 - (493 - 448 + 1)\ p + 493 = 0$
- $p^2 - 46\ p + 493 = 0$
  - Two roots are p=17, q=29
- Supposing the public exponent of Alice is e=3, find her private exponent d.
- $d=3^{-1} \bmod \Phi(n)=3^{-1} \bmod 448=299$
- d can be easily computed as $3^{\Phi(448)-1} \bmod 448 = 3^{191} \bmod 448$ =299 (square & multiply)

Factoring Large Numbers

- **RSA-640 bits, Factored Nov. 2 2005**
- **RSA-200 (663 bits) factored in May 2005**
- **RSA-768 has 232 decimal digits and was factored on December 12, 2009, latest.**
- Three most effective algorithms are
  – quadratic sieve
  – elliptic curve factoring algorithm
  – number field sieve

Fermat Factorization: example

- Let us suppose Alice publishes the following information (her public key):
  - n=6557, e=131
- If we assume p > q, we can always write:

$$n = y^2 - x^2 = \frac{(p+q)^2}{2^2} - \frac{(p-q)^2}{2^2}$$

An odd integer is the difference of 2 squares

- Fermat factorization is efficient if p ≅ q. In this case we have $y \cong \sqrt{n}\ and\ x \cong 0$

Exercise 2 - Fermat Factorization

- Let us try, in order, all integer numbers y> $\sqrt{n}$, calculating each time:
  $\hat{x}^2 = y^2$- n
- We go on until $\hat{x}^2$ is a perfect square
- In our example y> $\sqrt{n}$ = 80.9
- Let us try y=81. In this case we have
  $\hat{x}^2 = 6561$- 6557= 4
- In fact, n=6557 and 6557+2^2=81^2
  - p=81+2=83, q=81-2=79

- What is the private exponent of Alice?

Exercise 2 - solution

- $\Phi(n)=(p-1)(q-1)=6396$
- $e=131$
- – The private exponent of Alice is $d = e^{-1} \bmod \Phi(n) = 131^{-1} \bmod 6396$
- – $d=2783$
  - We can compute it also as follows (square & multiply):
  - $d = 131^{\Phi(6396)-1} \bmod 6396 = 131^{1920-1} \bmod 6396 = 131^{1919} \bmod 6396 = 2783$

Exercise 3 - Fermat Factorization

- Try to factor, using Fermat factorization, the following numbers:

- $n = 295927$
- $n = 213419$
- $n = 1707$

Exercise 3 - Solution

- Try to factor, using Fermat factorization, the following numbers:

- n = 295927
  - Sqrt(n)=543.99, and 544^2-n=9=3^2
  - Hence p = 544-3=541, q=544+3=547
- n = 213419
  - Sqrt(n)=461.79, and 462^2-n=25=5^2
  - Hence p = 462-5=457, q=462+5=467
- n = 1707
  - n=1707, 286^2-1707=283^2
  - … hence p=286+283=569, q=286-283=3

Exercise 4

- Let us consider an RSA Public Key Cryptosystem
- Alice publishes her public key, namely:
  - n=221
  - e (her public exponent), e=13
- Try to break Alice cryptosystem, factoring n

Exercise 4 - Solution

- Let us consider an RSA Public Key Cryptosystem
- Alice publishes her public key, namely:
  - n=221
  - e (her public exponent), e=13
- Try to break Alice cryptosystem, factoring n
  - p=13, q=17
  - $\Phi(n) = (p-1)(q-1) = 12*16+192$
  - Private exponent d: de=1 mod 192. Hence d=invmodn(13,192)=133

In practical situations, the « invmodn » function found here can be used http://www2.math.umd.edu/~lcw/MatlabCode/