Topics in Discrete Mathematics: Introduction to Mathematical Cryptography. Exercises.

Dan Fretwell

Spring semester 2021/22

Chapter 1 (Classical methods)

1. (a) Encrypt `DOG` using Caesar shift $k = 13$.

   (b) Decrypt `PBJ` using the same shift.

   (c)

   ```
   VZJXYNTSTSJFTSYMJJCFRBNQQGJFG
   TZYHQFXXNHFQJSHWDUYNTSRJYMTIX
   ```

   .

   (d) Can you find a meaningful word that Caesar shifts to another? Can you find a meaningful word that Caesar shifts to another meaning the same thing? (There is an easy example if you know basic French and English).

2. (a) Encrypt the word `SUBSTITUTION` using the permutation

   $$\sigma = (0\ 13)(1\ 14)(2\ 15)(3\ 16)...(12\ 25).$$

   (b) Decrypt the word `PVCURE` using σ.

   (c)

   ```
   SFB SFGLD EXNTS JGIB EL BWEK GR JGIB YNT LBUBQ JGIB ILNV
   JGIB VFES SFB PTBRSGNLR EQB JGIB NL. JGIB VFY AELS SFBY
   JGIB SBJJ TR JGIB VFES SN ILNV. PTBRSGNL NLB X NL SFB
   BWEK VGJJ XB NL RSTCC CQNK AFEOSBQR SVN SFQBB CNTQ ELM CGUB.
   ```

3. (a) Encrypt `GET SHIFTY` using Vigenere with keyword `RICK`.

   (b) Decrypt `BWTDJQ FZVI` using Vigenere with the keyword `MORTY`.

(c)

```
PFKQ AEEZ PFKQ ABRQ PFKQ CLU QZBR XMHE SSFNS XL LUOB TQPI
UE EYOGX NUQWQIAR LNQ G. NUQWQIAR LNQ G TIXP YE AR YOFL
ZHMTQEDW PIJ EKD EISEZ. XEEDI TIXP KO GRPEQR YIFW QO FLFS BEOT.
```

Chapter 2 (Diffie-Hellman)

1. (a) Show that $g = 2$ is a primitive root for $\mathbb{F}_{13}$.

   (b) Let p be prime. Prove that $g \in \mathbb{F}_p^\times$ is a primitive root if and only if $g^{\frac{p-1}{q}} \neq 1$ for each prime $q \mid p-1$ (i.e. you don't have to calculate all powers of g to decide whether g is a primitive root, just the "maximal" ones).

   (c) Use the previous part to show quickly that $g = 2$ is a primitive root for $\mathbb{F}_{29}$.

2. Alice and Bob wish to use Diffie-Hellman to create a shared key. They agree to use the primitive root $g = 2$ of $\mathbb{F}_{29}$. Alice chooses secret value $k_A = 10$ and Bob chooses secret value $k_B = 25$.

   (a) What information is sent between Alice and Bob?

   (b) What is their shared key? (Demonstrate that both Alice and Bob can compute this).

3. Suppose that g is a primitive root for $\mathbb{F}_p$. Alice chooses secret value satisfying $1 \leq k_A \leq \lfloor \log_g(p) \rfloor < p$ when using Diffie-Hellman with Bob. However, Eve was easily able to find their shared key. Why?

Chapter 3 (RSA)

1. (a) Use Inclusion-Exclusion to prove that $\phi(N) = N \prod_{\text{primes } p \mid N} \left(1 - \frac{1}{p}\right)$.

   (b) Find the values $\phi(24), \phi(25)$ and $\phi(26)$.

2. Alice and Bob wish to use RSA to communicate. Bob chooses secret primes $p = 5$ and $q = 17$ and $e = 11$.

   (a) What are Bob's public and private keys?

   (b) Alice wishes to send the message $m = 4$ to Bob. What encrypted message does she send?

   (c) Demonstrate that Bob can decrypt Alice's message.

3. Bob's public RSA key is (e, N) and Alice uses this to encrypt a message $1 \leq m < N^{\frac{1}{e}}$. She sends the encrypted message c to Bob but Eve intercepts it. She seems to have no trouble decrypting c. Why?

4. Explain why the following "large" semiprimes are bad choices for RSA public keys:

(a) $N = 1225782003978549292334378589543794217417466$.

(b) $N = 38691326126793$.

(c) $N = 1864968064455009946373230835946473859485543543845$.

Chapter 4 (ElGamal)

1. Compute the following discrete logs:

   (a) $\text{dlog}_4(13)$ in $\mathbb{Z}_{45}$ under addition.

   (b) $\text{dlog}_5(16)$ in $\mathbb{F}_{23}^{\times}$ under multiplication.

   (c) $\text{dlog}_A(B)$ in $\text{GL}_2(\mathbb{F}_7)$ under multiplication, with $A = \begin{pmatrix} 6 & 0 \\ 1 & 5 \end{pmatrix}$ and $B = \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}$.

2. Bob's public ElGamal key is $(\mathbb{F}_{13}^{\times}, 12, 2, 6)$.

   (a) Alice wishes to send the message $m = 9$ to Bob, using secret value $s = 3$. What is the encrypted message that she sends?

   (b) Bob's private key is $k = 5$ (since $2^5 \equiv 6 \bmod 13$). Demonstrate that Bob can decrypt Alice's message.

   (c) Other than the fact that $p = 13$ is too small for real life security, why is Alice's choice of s a bad choice? (See Q3 in Chapter 2).

Chapter 5 (Digital signatures)

1. Alice wishes to sign a document using the RSA signature scheme. Her public key is $(3, 33)$ and her private key is 7 (since $\phi(33) = 20$ and $3 \cdot 7 \equiv 1 \bmod 20$). Bob challenges her to decrypt the auxiliary message $m_0 = 14$.

   (a) What is the signature that Alice sends to Bob?

   (b) Demonstrate that Bob is able to verify the signature.

2. Alice wishes to sign a document using the ElGamal signature scheme. Her public key is $(\mathbb{F}_{17}^{\times}, 3, 5)$ and her private key is 5 (since $3^5 \equiv 5 \bmod 17$). She decides to use auxiliary message $m_0 = 7$ and secret value $s = 9$.

   (a) What is the signature that Alice sends to Bob?

   (b) Demonstrate that Bob is able to verify the signature.

3. Alice uses the ElGamal scheme to sign two different documents using the same public/private key and the same secret value s. Eve intercepts the two signatures and is able to gain access to Alice's private key k. How?

Chapter 6 (Knapsack)

1. Indicate which of the following sequences are superincreasing and solve the corresponding Knapsack Problems (using the greedy algorithm where possible).
   (a) 1,3,9,27,81,243 (111).
   (b) 1,5,7,14,25,53 (27).
   (c) 10,13,24,48,112, 211 (245).
   (d) 114,257,129,101,343,117 (461).

2. Let $a, b \geq 0$ and $n \geq 2$ be such that $a > bn$. Show that the the sequence $x_{m+1} = 2x_m - b$ with starting value $x_1 = a$ is a superincreasing sequence of length n.

3. Alice and Bob wish to use the Knapsack scheme to communicate. Bob chooses superincreasing sequence $1, 3, 8, 14, 30, 63$ and private key $(M, w) = (120, 53)$.
   (a) What is Bob's public key?
   (b) Alice wishes to send the bit string 011001 to Bob. What encrypted message does she send?
   (c) Demonstrate that Bob can decrypt Alice's message.

Chapter 7 (Secret sharing)

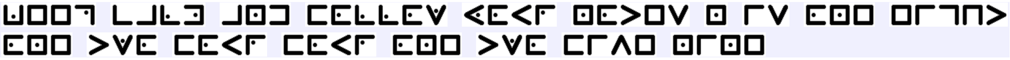
1. Use Lagrange Interpolation to find the equation of the unique cubic polynomial passing through the points $(1, 4), (2, 9), (3, 1), (4, 3)$ of $\mathbb{R}^2$.

2. Alice wishes to share the secret $S = 9 \in \mathbb{F}_{17}$ among $n = 6$ of her employees with threshold $t = 4$. She chooses polynomial $f(x) = 9 + 2x + 6x^2 + x^3$ and values $x_i = i$ for $1 \leq i \leq 6$.
   (a) What information will Alice distribute among her employees?
   (b) Demonstrate that four employees can retrieve the secret.

Cipher Challenge

The first person to break all of the ciphers below and email the full solution to `daniel.fretwell@bristol.ac.uk` will receive a prize.

```
TBBQJBEXOHGGURERFZBERGBQBLRGRVFFRIRAGRRA
```



$(1,2,3),(7,1,1),(1,1,1),(5,2,4),(7,2,7),(1,2,2),(4,1,1),(3,5,2),(4,3,1),$
$(2,1,6),(6,1,2),(1,1,5),(7,1,6),(6,2,4),(1,1,3),(4,2,1),(6,1,1),(2,1,5),$
$(1,1,2),(4,1,3),(2,1,1),(7,1,2),(5,3,4),(3,3,2),(1,2,1),(4,6,6),(7,4,2),$
$(5,2,4),(1,4,5),(1,4,3),(1,4,4),(6,5,3),(3,1,1),(7,5,1),(1,1,5),(7,1,4),$
$(7,4,1),(7,2,1),(3,2,1),(3,2,2),(3,2,3),(3,6,1),(3,6,2),(3,6,3),(4,6,2),$
$(2,3,2),(7,4,5),(4,7,3),(3,3,1),(4,6,6),(3,3,1),(5,3,3),(3,5,4),(1,4,6).$

```
VWCNRRWYLSROCBVQUUMVXAZGGFXGXTHWIFHHQJLLSKSJRNSVLIJQORWP
```