MATA02 – Winter 2022 – Lecture 12b Handout – Prof. Yun William Yu

Exercise instructions (groups of 3-5 people), example in sub bullets:

- Generate an RSA modulus n using 2-digit primes.
  - $p = 29, q = 31$, so $n = 899$.
- Choose an exponent k such that $\gcd(k, \phi(n)) = 1$.
  - $\phi(899) = 28 * 30 = 840$. Choose $k = 11$.
- Choose a Caesar cipher key $a > 1$. Make sure $\gcd(a, n) = 1$.
  - Let $a = 5$.
- Encrypt the Caesar cipher key to get $b \equiv a^k \pmod{n}$
  - $b \equiv 5^{11} \equiv 738 \pmod{n}$
- Write a short message of about 15-30 characters.
  - ILOVEMATHEMATICS
- Convert it to decimal-letter encoding:
  - Msg = 9 12 15 22 5 13 1 20 8 5 13 1 20 9 3 19
- Encrypt the message using the Caesar cipher:
  - Encrypted msg: 14 17 20 1 10 18 6 25 13 10 18 6 25 14 8 24
  - In letters: NQTAJRFYMJRFYNHX
- Send a message to the other groups: (n, k, b) and encrypted msg
  - $(899, 11, 738)$, NQTAJRFYMJRFYNHX

Then, after everyone's sent out messages via chat, everyone is going to decrypt the other groups' messages.

- Decrypt RSA by computing $a \equiv \sqrt[k]{b} \pmod{n}$.
  - $\sqrt[11]{738} \pmod{899} \equiv 5$.
- Then use the Caesar cipher key to decrypt the message
  - NQTAJRFYMJRFYNHX – 5 = ILOVEMATHEMATICS

List of primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
14	15	16	17	18	19	20	21	22	23	24	25	26

Caesar cipher:

1. Choose a key between 1 and 25.
2. Add this number to the decimal-encoded letters of the message in mod 26.
3. Convert the decimal-encoded letters back to letters.
4. To decrypt, reverse by subtracting instead of adding the key.

RSA algorithm:

1. Alice says hello to Bob.
2. Bob chooses two large prime numbers p, q and computes $n = pq$.
3. Bob chooses an exponent k, such that $\gcd\big(k, \phi(n)\big) = 1$.
4. Bob sends (n, k) to Alice as a public key.
5. Alice has a message a, where $\gcd(a, n) = 1$.
   She sends $b \equiv a^k \pmod{n}$ to Bob.
6. Bob decrypts the message by computing $a \equiv \sqrt[k]{b} \pmod{n}$.

Hybrid cryptosystem:

1. Use RSA to send a key for a Caesar cipher.
2. Then once both parties know the key, send later messages using the Caesar cipher with that key instead.