

Comment (2024): in 2019, four-function calculators were permitted on the exam, so slightly more complicated arithmetic was involved and no modular arithmetic reference tables are provided. This year, calculators will not be permitted; instead reference tables like those on the 2020 exam will be provided.

1. (a) [5 points] Find integers  $u$  and  $v$  such that  $101u + 80v = 1$ . Clearly show the process you have used to compute them.
- (b) [2 points] Determine  $80^{-1} \pmod{101}$ .
- (c) [5 points] Solve the following pair of congruences. Your answer should be a single congruence that describes *all* possible solutions.

$$\begin{aligned}n &\equiv 2 \pmod{80} \\n &\equiv 7 \pmod{101}\end{aligned}$$

2. [7 points] Alice and Bob are performing Diffie-Hellman key exchange (see back page for the textbook's reference table) with parameters

$$p = 103, g = 5.$$

For her secret number  $a$ , Alice chooses

$$a = 33.$$

Determine Alice's public number  $A$ . Clearly show the process you use to compute it; for full points you should use a process that would scale well to larger primes.

3. [7 points] Alice and Bob are using ElGamal encryption (see back page for the textbook's reference table), with the following public parameters.

$$p = 31, g = 3.$$

Alice publishes the following public key.

$$A = 22$$

Use the Babystep-Giantstep Algorithm (Shanks's algorithm) to determine Alice's private key  $a$ . Clearly show all steps, including the two lists that you use to check for a collision.

4. Let  $p$  be a prime number, and  $g$  an element of  $(\mathbb{Z}/p\mathbb{Z})^*$ .
  - (a) [3 points] Define what it means for  $g$  to be a *primitive root* modulo  $p$ .
  - (b) [3 points] Prove that if  $g$  is a primitive root modulo 29, then  $g^8 \pmod{p}$  has order 7.
  - (c) [3 points] Prove that if  $g$  is a primitive root modulo 29, then  $g^3$  is also a primitive root modulo 29.

Reference tables from textbook:

Public parameter creation	
A trusted party chooses and publishes a (large) prime $p$ and an integer $g$ having large prime order in $\mathbb{F}_p^*$ .	
Private computations	
Alice	Bob
Choose a secret integer $a$ . Compute $A \equiv g^a \pmod{p}$ .	Choose a secret integer $b$ . Compute $B \equiv g^b \pmod{p}$ .
Public exchange of values	
Alice sends $A$ to Bob $\xrightarrow{\hspace{2cm}}$ $A$ $B$ $\xleftarrow{\hspace{2cm}}$ Bob sends $B$ to Alice	
Further private computations	
Alice	Bob
Compute the number $B^a \pmod{p}$ . The shared secret value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$ .	Compute the number $A^b \pmod{p}$ .

Table 2.2: Diffie–Hellman key exchange

Public parameter creation	
A trusted party chooses and publishes a large prime $p$ and an element $g$ modulo $p$ of large (prime) order.	
Alice	Bob
Key creation	
Choose private key $1 \leq a \leq p - 1$ . Compute $A = g^a \pmod{p}$ . Publish the public key $A$ .	
Encryption	
	Choose plaintext $m$ . Choose random element $k$ . Use Alice's public key $A$ to compute $c_1 = g^k \pmod{p}$ and $c_2 = mA^k \pmod{p}$ . Send ciphertext $(c_1, c_2)$ to Alice.
Decryption	
Compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$ . This quantity is equal to $m$ .	

Table 2.3: Elgamal key creation, encryption, and decryption