Key Establishment

1. The discrete-logarithm problem in the additive group $\mathbb{Z}_p$ is to find a solution to the modular equation $A = g \cdot a \bmod p$, where a is unknown. But this is easy: $a = Ag^{-1} \bmod p$. Note that the computing the multiplicative inverse is very efficient when using the Extended Euclidean Algorithm.

2. Since $q \mid p-1$ we have $p-1 = rq$ and thus $p = rq+1$, where r is even. First, generate a random prime q of length n_q. Choose an even uniform integer r of length $n_p - n_q$ and set $p = rq+1$. Then p has the required bit length n_p. Check the primality of p and choose a new integer r if p is not a prime number. To find a generator g with $\text{ord}(g) = q$, choose a random number h in the range $1 < h < p-1$ and compute $g = h^r \bmod p$. If $g \equiv 1 \bmod p$, choose another h. If $g \not\equiv 1 \bmod p$, then we have $\text{ord}(g) = q$. Note that the definition of g yields $\text{ord}(g) \mid \frac{p-1}{r} = q$. Since q is a prime, $\text{ord}(g)$ must be either q or 1.

3. $G = \langle 2 \rangle$ is a subgroup of $\mathbb{Z}_{89}^*$ and $\text{ord}(G) = \text{ord}(2) \mid 88$. Since $2^{11} \equiv 1 \bmod 89$ and 11 is a prime, one has $\text{ord}(2) = 11$. The Diffie-Hellman shared key k is an element of G. Therefore, 11 different keys can occur in this case.

4. a) $p = 43$ and $g = 3$ are given. Then $p-1 = 42 = 2 \cdot 3 \cdot 7$. Compute $g^{\frac{p-1}{q}} \bmod p$ for all prime divisors q of $p-1$. We get $3^{21} \equiv 42$, $3^{14} \equiv 36$ and $3^6 \equiv 41 \bmod 43$. None of these values is congruent to 1, and so the order of g must be maximal, i.e., $\text{ord}(g) = 42$.
   b) You send Alice the public key $B = g^b = 3^{26} \equiv 15 \bmod 43$. The shared secret key is $k = A^b = 14^{26} \equiv 23 \bmod 43$.

5. a) $\text{ord}(\mathbb{Z}_{107}^*) = 106 = 2 \cdot 53$. Let $g \equiv 3$. Since $g^{53} \bmod 107 \equiv 1$, we have $\text{ord}(g) = 53$, which is a prime number.
   b) Since $\lfloor \sqrt{53} \rfloor = 7$, at most 7 babysteps and 7 giantsteps, i.e., ≤ 14 exponentiations are necessary.
   c) We have $m = 7$ and $A = 12$. Firstly, compute the babysteps $Ag^{-r} \bmod p$, where $r = 0, 1, \ldots, 6$:
   $$12, 4, 37, 48, 16, 41, 85$$
   Secondly, compute $T = g^7 \bmod 107 \equiv 47$ and the giantsteps $T^s \bmod p$, where $s = 0, 1, \ldots, 7$:
   $$1, 47, 69, 33, 53, 30, 19, 37.$$
   We have a match for $r = 2$ (babystep) and $s = 7$ (giantstep). Hence $a = ms + r = 51$ and $\log_3(12) = 51$.

6. Use SageMath. The hexadecimal strings defining p, g and q can be copied from RFC 5114, Section 2.3. First, check the primality of p and q.

```
sage: ps='87A8E61D B4B6663C FFBBD19C 65195999 8CEEF608 660DD0F2\
       5D2CEED4 435E3B00 E00DF8F1 D61957D4 FAF7DF45 61B2AA30\
       16C3D911 34096FAA 3BF4296D 830E9A7C 209E0C64 97517ABD\
       5A8A9D30 6BCF67ED 91F9E672 5B4758C0 22E0B1EF 4275BF7B\
       6C5BFC11 D45F9088 B941F54E B1E59BB8 BC39A0BF 12307F5C\
       4FDB70C5 81B23F76 B63ACAE1 CAA6B790 2D525267 35488A0E\
       F13C6D9A 51BFA4AB 3AD83477 96524D8E F6A167B5 A41825D9\
       67E144E5 14056425 1CCACB83 E6B486F6 B3CA3F79 71506026\
       C0B857F6 89962856 DED4010A BD0BE621 C3A3960A 54E710C3\
```

```
       75F26375 D7014103 A4B54330 C198AF12 6116D227 6E11715F\
       693877FA D7EF09CA DB094AE9 1E1A1597'
sage: p=ZZ(ps,16)
sage: p.is_pseudoprime()
True
sage: qs = '8CF83642 A709A097 B4479976 40129DA2\
       99B1A47D 1EB3750B A308B0FE 64F5FBD3'
sage: q=ZZ(qs,16)
sage: q.is_prime()
True
```

Next, we verify that $g^q \equiv 1 \bmod p$ so that $\mathrm{ord}(g) \mid q$. Since $g \not\equiv 1$ and q is prime, we conclude that $\mathrm{ord}(g) = q$.

```
sage: gs='3FB32C9B 73134D0B 2E775066 60EDBD48 4CA7B18F 21EF2054\
       07F4793A 1A0BA125 10DBC150 77BE463F FF4FED4A AC0BB555\
       BE3A6C1B 0C6B47B1 BC3773BF 7E8C6F62 901228F8 C28CBB18\
       A55AE313 41000A65 0196F931 C77A57F2 DDF463E5 E9EC144B\
       777DE62A AAB8A862 8AC376D2 82D6ED38 64E67982 428EBC83\
       1D14348F 6F2F9193 B5045AF2 767164E1 DFC967C1 FB3F2E55\
       A4BD1BFF E83B9C80 D052B985 D182EA0A DB2A3B73 13D3FE14\
       C8484B1E 052588B9 B7D2BBD2 DF016199 ECD06E15 57CD0915\
       B3353BBB 64E0EC37 7FD02837 0DF92B52 C7891428 CDC67EB6\
       184B523D 1DB246C3 2F630784 90F00EF8 D647D148 D4795451\
       5E2327CF EF98C582 664B4C0F 6CC41659'
sage: g=ZZ(gs,16)
sage: power_mod(g,q,p)
1
```

7. $g^2A^1 = g^5A^5 \equiv 26 \bmod 59$. Then $a = \frac{5-2}{1-5} \equiv 3 \cdot 7 = 21 \bmod 29$. In fact, $g^a \bmod q = 4^{21} \bmod 59 \equiv 9 = A$.

8. $\mathrm{ord}(\mathbb{Z}^*_{109}) = 108 = 2^2 \cdot 3^3$. Since $11^{108/2} \bmod 109 \not\equiv 1$ and $11^{108/3} \bmod 109 \not\equiv 1$, $g = 11 \bmod 109$ is a generator of $G = \mathbb{Z}^*_{109}$.
   G is isomorphic to the product $G_1 \times G_2$, where G_1 is cyclic of order 4 and G_2 is cyclic of order 27, respectively. The generator $g = 11 \in G$ is mapped to
   $$(g_1,\, g_2) = (11^{27} \bmod 109,\ 11^4 \bmod 109) = (76, 35) \in G_1 \times G_2.$$
   Accordingly, $A = 54$ is mapped to $(A_1, A_2) = (33, 75)$. Next, we determine the discrete logarithm in the smaller groups G_1 and G_2: $\log_{76}(33) = 3$ and $\log_{35}(75) = 12$. The discrete logarithm a in the full group G satisfies $a \equiv 3 \bmod 4$ and $a \equiv 12 \bmod 27$. The Chinese Remainder Theorem gives $a \equiv 39 \bmod 108$, and in fact $11^{39} \bmod 109 \equiv 54$.

9. Without the hashing we would have $k = s$, i.e., the key is the RSA plaintext. In a CPA experiment for RSA key encapsulation an adversary could simply test a challenge k' by computing $(k')^e \bmod N$ and compare the result with c. If they are equal, then $k = k'$ and the adversary outputs $b' = 1$. Otherwise, k' is random and the adversary outputs $b' = 0$. The adversary wins the experiment, and so the modified scheme is insecure.

10. If a and b are both re-used, then the shared Diffie-Hellman key $k = g^{ab}$ remains constant. If a is re-used and b is fresh, then a new shared secret key k is

generated. However, if a long-term private key a is compromised, then the consequences are severe: the shared secret keys of all Diffie-Hellman exchanges which used a can be easily computed. In order to achieve *perfect forward secrecy* (PFS), both Diffie-Hellman keys a and b must be ephemeral.

11. A Man-in-the-Middle (Mallory) runs separate Diffie-Hellman exchanges with Alice and Bob. In the exchange with Alice he masquerades as Bob and in the exchange with Bob he masquerades as Alice. Mallory generates private keys a' and b'. He intercepts the message A from Alice and sends his own public key $A' = g^{a'}$ to Bob. Accordingly, he intercepts B from Bob and sends $B' = g^{b'}$ to Alice. Then Mallory's shared secret key with Alice is $k_A = A^{b'}$ and the shared secret key with Bob is $k_B = B^{a'}$. Alice and Bob cannot detect this attack, unless they are able to verify the authenticity of the public keys A and B.

12. a) Let $(c_1, c_2) = (g^b, A^b m)$ be an ElGamal ciphertext. Decryption is correct:

$$c_1^{-a} c_2 = g^{-ab} A^b m = g^{-ab} g^{ab} m = m.$$

b) $m = 17^{-20} \cdot 16 \equiv 25 \cdot 16 \equiv 46 \bmod 59$.

c) If an adversary knows b and eavesdrops a ciphertext (c_1, c_2), then they can use the equation $c_2 = A^b \cdot m$ to compute the plaintext $m = c_2 A^{-b}$ without knowing the secret key a.

If b is re-used, then the encryption is no longer randomized. Furthermore, $A^b = c_2 m^{-1}$ can be derived from any known plaintext/ciphertext pair. Suppose a new plaintext m' is encrypted using the same secret parameter b. Then decryption is easy since $m' = c_2 (A^b)^{-1}$.