HW 2 Answers - Ray Li

CSCI-UA.0480-63

October 8, 2025

1. Public key crypto at toy security levels

(a) $p = 10007$, $g = 3$

1. Order of $g \bmod p$: 5003.
2. Shamir three-pass with $m = 1337$, $a = 2461$, $b = 4319$:
   - $a^{-1} \bmod (p-1) = 7103$, $b^{-1} \bmod (p-1) = 5259$.
   - Transmissions: $x_1 = m^a \bmod p = 792$, $x_2 = x_1^b \bmod p = 1441$, $x_3 = x_2^{a^{-1}} \bmod p = 5629$ (Bob recovers m by raising to b^{-1}).
3. Diffie–Hellman with $a = 2461$, $b = 4319$:
   - $A = g^a \bmod p = 5974$, $B = g^b \bmod p = 7413$, shared secret $s = B^a \bmod p = A^b \bmod p = 6122$.

(b) RSA with $p = 383$, $q = 401$

1. $\varphi(N) = (p-1)(q-1) = 152800$.
2. With $e = 11$, the private exponent $d \equiv e^{-1} \bmod \varphi(N) = 13891$.
3. Encrypting 1337: $c = m^e \bmod N = 113846$.
4. Signing 1337: $\sigma = m^d \bmod N = 101732$.

2. Digital signatures

Most signature schemes sign a fixed-size value (usually a hash). If Alice signs each 1024-bit block with DSA and concatenates the signatures, it is insecure.

Why this is insecure

- Without hashing, the scheme is malleable. An attacker can splice blocks from two messages that Alice signed and produce a new message whose per-block signatures all verify. - There is no binding across blocks. DSA.Sign(m_1) $\|$ DSA.Sign(m_2) does not prove Alice signed the whole message—only that she once signed each block individually, possibly in a different context. - Length and formatting are not covered. Reordering, deleting, or duplicating blocks still passes verification.

Concrete forgery

Suppose Alice signed two distinct 1024-bit blocks x and y, producing (σ_x, σ_y). Consider the forged message M' = $x \parallel y$. Its "signature" $\sigma' = \sigma_x \| \sigma_y$ verifies under Alice's key on M' in this broken scheme, even if Alice never signed M' as a whole. More generally, if Alice signed blocks x1,...,xk at any time, an attacker can assemble any message made of those blocks and concatenate the corresponding signatures, yielding a valid-looking overall signature.

Fix

Sign a collision-resistant hash of the whole message: $\sigma = \mathrm{Sign}(H(M))$. This binds all content, order, and length into one digest and prevents block-wise cut-and-paste.

3. Signatures with related secret values

We look at El Gamal signatures with $r = g^y \pmod p$ and $s = (m - rx) \cdot y^{-1} \pmod{p-1}$. If two different messages $m_1 \neq m_2$ are signed using the same nonce y (so the same r), we can recover the private key x as follows.

Attack when the same r is reused

Given (r, s_1) on m_1 and (r, s_2) on m_2:

$$s_1 \equiv (m_1 - rx) \cdot y^{-1} \pmod{p-1}$$
$$s_2 \equiv (m_2 - rx) \cdot y^{-1} \pmod{p-1}$$

Subtract the equations to eliminate x:

$$(s_1 - s_2) \equiv (m_1 - m_2) \cdot y^{-1} \pmod{p-1}.$$

Provided $\gcd(s_1 - s_2, p-1) = 1$, invert to get

$$y \equiv (m_1 - m_2) \cdot (s_1 - s_2)^{-1} \pmod{p-1}.$$

Plug back (e.g., into the first) to solve for x:

$$rx \equiv m_1 - s_1 y \pmod{p-1} \quad \Rightarrow \quad x \equiv r^{-1} \cdot (m_1 - s_1 y) \pmod{p-1}.$$

So, if you reuse the signing nonce, the secret key can be found.

4. Reductions: CDH implies DDH

We are given an oracle A_{CDH} that on input (g, p, g^a, g^b) outputs g^{ab} with probability P (non-negligible). Construct a distinguisher A_{DDH} for inputs (g, p, g^a, g^b, h):

Distinguisher A_{DDH}

1. Query A_{CDH} on (g, p, g^a, g^b) to obtain z.
2. Compare z to h. If $z = h$, output "DDH instance is real" (i.e., $h = g^{ab}$); otherwise output "random".

Correctness and advantage

If the instance is real ($h = g^{ab}$), then with probability P we have $z = g^{ab} = h$ and A_{DDH} outputs "real"; otherwise it guesses "random". If the instance is random ($h \leftarrow \mathbb{Z}_p^*$), then $z = g^{ab}$ is independent of h, so $\Pr[z = h] = 1/(p-1)$ (negligible), and A_{DDH} outputs "random" with overwhelming probability. Overall,

$$\Pr[\text{output real} \mid h = g^{ab}] \geq P, \qquad \Pr[\text{output real} \mid h \leftarrow \mathbb{Z}_p^*] \approx 0.$$

Thus A_{DDH} distinguishes with advantage at least $P - 1/(p-1)$ over $1/2$, which is non-negligible. Therefore, if CDH is easy, then DDH is easy; contrapositive: if DDH is hard, then CDH is at least as hard (CDH implies DDH, CDH is the stronger assumption).