# ECS 127 — Midterm 1 Solutions — Spring 2024

1. For *Diffie-Hellman secret-key exchange* we fixed a large prime number $p$ and a generator $g$ for $\mathbb{Z}_p^*$ (the multiplicative group of integers mod $p$). What follows is then done in that group: Alice selects $a \twoheadleftarrow \{1, 2, \ldots, p-1\}$ and computes $A = g^a$. She sends $A$ to Bob. Bob selects $b \twoheadleftarrow \{1, 2, \ldots, p-1\}$ and computes $B = g^b$. He sends $B$ to Alice. The parties will share $K = g^{ab}$, which Alice learns by computing $\boxed{B^a}$ and Bob learns by computing $\boxed{A^b}$ .

2. Suppose Alice encrypts a message $M \in \{0, 1, \ldots, 99\}$ to a ciphertext $C = M + K \pmod{100}$ using a uniformly random key $K \in \{0, 1, \ldots, 127\}$. This is the only message ever sent using the key $K$. The method $\boxed{\text{doesn't}}$ achieve perfect privacy. For example, $\Pr[C = 0 \mid M = 0] = \boxed{2/128}$ and $\Pr[C = 0 \mid M = 42] = \boxed{1/128}$

3. In our class, $R \twoheadleftarrow S$ means

   $\boxed{R \text{ is chosen (uniformly) at random from (the finite set or distribution) } S}$

   while $\mathcal{A}(R) \Rightarrow 1$ means $\boxed{\text{(the event that) } A\text{, on input } R\text{, outputs } 1}$

4. Recall the DES algorithm, DES: $\{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$. Name two of its **undesirable** characteristics and, for each, explain *why* the attribute is undesirable.

   a. the 56-bit key space is too small, making exhaustive key-search practical

   b. the design criteria were secret, which damaging trust in the algorithm.

   c. the hardware-centric design is slow in software and decreases how much the algorithm is used.

   d. Could have been better designed to withstand linear cryptanalysis, which wasn't know at the time of the algorithm's design. Better S-boxes could have fixed this.

   e. *Not discussed in class, but inferable from things said in class:* The 64-bit blocksize is inconveniently small, opening the door for practical birthday attacks when the algorithm is used in conventional modes.

   f. *Not discussed in class:* It's hard to implement in SW without big tables, which can have cache effects and result in data-dependent running times, enabling some cryptanalysis.

5. Define a blockcipher $E\colon \{0,1\}^{256} \times \{0,1\}^{128} \to \{0,1\}^{128}$ that does a great job of concealing the key—no adversary can do well at guessing it—yet $E$ is, nonetheless, totally insecure in the ind-sense. $\boxed{E_K(X) = X}$

6. The number of permutations on $\{0,1\}^{128}$ is $|\text{Perm}(128)| = \boxed{2^{128}!}$ The number of cycles on $\{0,1\}^{128}$ is $|\text{Cycl}(128)| = \boxed{(2^{128} - 1)!}$

7. You are working in GF($2^8$), the finite field with $2^8$ points, representing points using the irreducible polynomial $g(\mathtt{x}) = \mathtt{x}^8 + \mathtt{x}^4 + \mathtt{x}^3 + \mathtt{x} + 1$. What point will you get if you square $s = \mathtt{00010000} = \mathtt{x}^4$ ? Write it in binary. $\boxed{\mathtt{x}^8 = 00011011}$

8. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher. Suppose you design a PRG $G : \{0,1\}^k \to \{0,1\}^\infty$ that depends on $E$. You want to prove that if $E$ is a secure PRP then $G$ is a secure PRG. To do this you would need to provide a *reduction*. The reduction will start with an adversary $A$ that attacks $\boxed{G}$ and will transform it into an adversary $B$ that attacks $\boxed{E}$. You'll then prove that if $\boxed{\mathbf{Adv}_G^{\mathrm{prg}}(A)}$ is large then $\boxed{\mathbf{Adv}_E^{\mathrm{prp}}(B)}$ is large, too.

9. In a homework solution we applied Shamir secret-sharing byte-wise to a message $M = M_1 \cdots M_m$, each $M_i \in \{0,1\}^8$. In what way was that approach better than just applying Shamir's scheme directly to $M$?

   It more simpler and more efficient to work in GF($2^8$) than to work in some potentially *huge* finite field that contains a point representing $M$.

   Sketch an alternative method to secret-share $M = M_1 \cdots M_m$ that requires the dealer to only use Shamir secret-sharing on a 32-byte string. The dealer ...

   shares out a uniformly 32-byte random key $K$ *and* a ciphertext $C \leftarrow \mathcal{E}_K(M)$ that is an encryption of $M$ under $K$. One way to do the encryption would be $C \leftarrow G(K) \oplus M$ for a PRG $G$ stretching 32-bytes to $|M|$ bits.

10.1) ✓ In an ind-secure symmetric encryption scheme, an encryption of `Hello` and an encryption of `mom` might be easy for an adversary to tell apart. *These are strings of different lengths*

20.2) ✓ In an ind-secure symmetric encryption scheme, ciphertexts might always start with the word `ciphertext`.

30.3) ✓ Parties $A$, $B$, and $C$ securely compute their average salary $s$. Then $A$ will necessarily learn, in addition to $s$, the average salary $s_{BC}$ of parties $B$ and $C$.

40.4) ☐ ind-security implies ind\$-security (indistinguishability from random bits).

50.5) ☐ Perfect privacy, discussed near the beginning of our class, is the strongest possible notion of encryption-scheme security.

60.6) ✓ If an encryption scheme's key space is smaller than its message space, it can't achieve perfect privacy.

70.7) ☐ ChaCha20 has been proven secure: we know that reasonable adversaries have small prp-advantage in attacking it. *I mean to write prf-advantage, but it doesn't really matter: primitives like ChaCha20 don't themselves have any sort of provably-security claims.*

80.8) ✓ If an asymptotically secure PRG exists than P≠NP.

90.9) ✓ DES would remain invertible even if each S-box were replaced by the function $S(x_1x_2x_3x_4x_5x_6) = (x_1 + 2x_2 + 3x_3 + 5x_4 + 7x_5 + 11x_6) \bmod 16$ (treated as a 4-bit string).

100.10) ✓ On a homework we saw that, experimentally, RC4's output *is* distinguishable from truly random bits.

110.11) ✓ If $E : \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$ has good security as a PRP then it has good security as a PRF. *This is the PRP/PRF switching lemma; you're good until nearly* $\sim 2^{128}$*queries, which is enormous.*

120.12) ☐ CBC-mode encryption with a counter IV is ind-secure if its underlying blockcipher is prp-secure. *ind-security but not ind$-security*

130.13) ☐ Adversary $\mathcal{A}$ queries a random function $f \twoheadleftarrow \{0,1\}^{128}$ at $2^{80}$ different points. The answers returned are probably all distinct (different from one another).

140.14) ☐ An *oracle* $\mathcal{O}$ computes some deterministic function $f$ of the query $X$ it is asked; it immediately returns $f(X)$. *Oracles are more general than functions: they can be stateful and probabilistic.*

150.15) ☑ The following exemplifies a *hybrid argument*: Let $\Pr[A^{\mathcal{O}_1} \Rightarrow 1] - \Pr[A^{\mathcal{O}_0} \Rightarrow 1] = \delta$. Then for any oracle $\mathcal{O}$ you devise, either $\Pr[A^{\mathcal{O}_1} \Rightarrow 1] - \Pr[A^{\mathcal{O}} \Rightarrow 1] \geq \delta/2$ or $\Pr[A^{\mathcal{O}} \Rightarrow 1] - \Pr[A^{\mathcal{O}_0} \Rightarrow 1] \geq \delta/2$.

160.16) ☑ CTR mode encryption and CBC mode encryption are both *malleable*.