PakCrypt National Cryptography Competition
Practice Problem Vol 1 — Online Rounds 1 & 2

PakCrypt Technical Design Committee

NCCS - Air University, Islamabad
pakcryptcircle@gmail.com

Abstract. This compendium provides some practice problems for the National Cryptography competition, covering the two online qualifying rounds across both competition tracks: the **Amateur** track (participants under 20) and the **Professional** track (open to all). The Amateur track emphasises reasoning, pattern recognition, and classical pen-and-paper cryptanalysis requiring no programming. The Professional track focuses on applied cryptography—RSA, Diffie–Hellman, hashing, block-cipher modes, and modern attacks—with compact numeric examples solvable by hand or with a basic calculator.
NOTE: The questions appearing in the actual PakCrypt competition may differ significantly from these sample questions. The provided samples are intended solely for practice and familiarization.

How to Use This Document

Problems are grouped by track and round. Within each section, difficulty rises from *Intro* through *Easy*, *Medium*, and *Hard*. The italic tag beside each problem title names its topic and difficulty. Every problem is followed by a green **solver hint**: a nudge toward the right technique, never the solution itself.

A note on calculators and tools. Amateur-track problems require only pencil, paper, and clear thinking. Professional-track problems may involve modular arithmetic with small numbers; a basic (non-programmable) calculator is sufficient and no computer is needed for the online rounds.

Table of Contents

1 Amateur Track (Under 20): Classical Cryptanalysis & Reasoning

1.1 Round 1

A01. A Gentle Start

Caesar / Shift • Intro

Each letter has been shifted forward by a fixed amount. Recover the message:

`DLSJVTL AV AOL UHAPVUHS JYFWAV VSFTWPHK`

Solver hint. Only 25 shifts exist. The commonest three-letter word in English is THE; find a group that becomes a common word under one fixed shift, then apply it everywhere.

A02. Clockwork

Caesar / Shift • Intro

A shift cipher hides a meeting place. Decrypt:

`FXXM FX TM MAX HEW VEHVD MHPXK TM GHHG`

Solver hint. Slide one alphabet against another. A doubled ciphertext letter often matches a common double such as EE or OO.

A03. Mirror, Mirror

Atbash • Intro

The alphabet is reversed (A↔Z, B↔Y, ...). Decode:

`GSV JFRXP YILDM ULC QFNKH`

Solver hint. This cipher is its own inverse. Reverse-map each letter and read off.

A04. Count the Letters

Monoalphabetic Substitution • Easy

A simple substitution conceals a hint about how to beat it:

`OMTLSTIYX CICGXNDN DN QBT FTX QJ RMTCFDIA NSRNQDQSQDJI`

Solver hint. Tally each ciphertext letter. The most frequent very likely is E. Spot a one-letter word (A or I) and the recurring three-letter THE.

A05. Odd One Out

Logic & Patterns • Easy

Four words share a hidden property; one does not. Which, and why?

`STRESSED, DESSERTS, REWARD, DRAWER, LEVEL`

Solver hint. Write each word backwards. Four become a different ordinary word; one becomes itself.

A06. Dots and Dashes

Morse Code • Easy

Decode (word breaks marked '/'):

`... . -. -.. .... . .-.. .-. / -. -- .-. - .... -. .- - .`

Solver hint. E is one dot, T one dash. Build outward from the shortest codes using a Morse chart.

A07. By the Numbers

Encodings (A1Z26) • Easy

Letters became their alphabet positions (A=1,...,Z=26):

`1-20-20-1-3-11 1-20 4-1-23-14`

Solver hint. Largest value is 26. Convert each number back: 1→A, etc.

A08. Grid Reference

Polybius Square • Medium

A standard 5×5 grid (I/J share a cell) turned each letter into row–column digits:

`51241344344254`

Solver hint. Draw the grid (A–E row 1, F–K row 2 with I/J, ...). Read digit pairs as (row, column).

A09. Zigzag

Transposition (Rail Fence) • Medium

Letters were written in a zigzag over 3 rails, then read row by row:

`TAAISHYRWTHNUEECG`

Solver hint. Count letters per rail by drawing the zigzag for the known length; deal ciphertext back into rows and read the zigzag.

A10. Backwards Day

Logic & Patterns • Easy

Each word is reversed and spaces removed. Recover the sentence:

`EHTYEKSIREDNUEHTTAM`

Solver hint. Reverse the whole string, then find natural word boundaries.

A11. Halfway Around

Caesar / ROT13 • Easy

A very common shift of exactly 13 was used (its own inverse). Decode:

`XABJYRQTR VF CBJRE THNEQ VG JRYY`

Solver hint. Shifting by 13 twice returns the original. Apply a shift of 13 to each letter.

A12. Operation Eagle

Monoalphabetic Substitution • Medium

Break this substitution cipher:

```
RBO OPAFO FPIHQ PR GCHICABR
```

Solver hint. Use letter frequencies plus word lengths. A lone repeated three-letter word starting many phrases is often THE; the double letter is a strong clue.

A13. Four-Letter Rhythm

Vigenère • Medium

A Vigenère cipher with a short keyword (a 4-letter word, a type of stronghold) was used:

```
ISWXSR KAJ SRLY KREQ CW MMS TTXHCX
```

Solver hint. With a 4-letter key, every 4th letter shares one shift. The theme (stronghold) narrows guesses; test FORT.

A14. Hidden in Plain Sight

Logic & Patterns • Medium

Read the first letter of each word to reveal a message:

```
Every Nice Cat Random Yields Pretty Tunes
```

Solver hint. NR.

A15. Multiply and Add

Affine • Hard

An affine cipher $E(x) = (5x + 8) \bmod 26$ (A=0) was applied. Recover the plaintext:

```
MAAX LESG UALJCP
```

Solver hint. Decryption is $D(y) = 5^{-1}(y-8) \bmod 26$. First find the inverse of 5 modulo 26 (it is 21).

A16. Next in Line

Number Patterns • Easy

What number continues the sequence, and what is the rule?

```
2, 3, 5, 7, 11, 13, ?
```

Solver hint. These are not arithmetic or geometric. Ask what property 2,3,5,7,11,13 all share.

A17. Fibonacci's Friend

Number Patterns • Easy

Find the next term and the rule:

`1, 1, 2, 3, 5, 8, 13, ?`

Solver hint. Add adjacent terms and compare with the next.

A18. Silent Spaces

Morse Code • Medium

This Morse message has NO separators between letters at all—only the raw dots and dashes (spaces shown are cosmetic; ignore them). Find a valid English two-word phrase:

`-.....-.-.-.-`

Solver hint. Without separators, many readings exist. Try splitting so that early letters form THE, a very common opener, then continue greedily.

A19. Three Columns

Columnar Transposition • Hard

A columnar transposition with keyword KEY (3 columns) was used; padding letter is X. Recover the message:

`ETKDNWTCTWAAAAX`

Solver hint. KEY orders columns as E<K<Y ⇒ read order 2,1,3. Rebuild the grid: total letters give the number of rows; place columns back in keyword order.

A20. Vowel Trouble

Logic & Patterns • Easy

All vowels were removed from a famous phrase. Restore it:

`KNWLDG S PWR`

Solver hint. Insert vowels to form real words. Word lengths and consonant skeletons strongly constrain the answer.

A21. Falcon Down

Caesar / Shift • Easy

Shift cipher. Decrypt:

`YMJ UFXXBTWI NX KFQHTS SNSJ`

Solver hint. Find the shift that turns a frequent three-letter group into THE.

A22. Quiet Place

Monoalphabetic Substitution • Medium

Solve the substitution:

`JAAQ ZQ QDA IFEOZOX`

Solver hint. Short words first: two-letter AT/TO/OF, three-letter THE. Pencil in guesses and propagate.

A23. Ones and Zeros

Binary / ASCII • Medium

Each group of bits is the binary ASCII code of one character:

`1001000 1001001`

Solver hint. Convert each binary number to decimal, then read it as an ASCII code (capital letters start at 65).

A24. Progressive Shift

Logic & Patterns • Medium

Each letter was shifted by a different amount: the 1st letter by 1, the 2nd by 2, the 3rd by 3, and so on. Recover the word:

`BVWEHQ`

Solver hint. To undo it, subtract 1 from the first letter, 2 from the second, 3 from the third, etc. (wrapping around Z to A).

A25. Two Rails

Transposition (Rail Fence) • Easy

A 2-rail rail fence. Decode:

`FENWLILSLEOALSOT`

Solver hint. With 2 rails the letters split into odd positions (rail 1) and even positions (rail 2). Interleave them back.

A26. Triangular Thinking

Number Patterns • Hard

Next term and rule:

`1, 3, 6, 10, 15, ?`

Solver hint. NR.

A27. Reflections

Atbash • Easy

Atbash. Decode:

`TFZIW GSV TLOW`

Solver hint. A↔Z. Apply the reversal; it undoes itself.

A28. Three-Letter Key

Vigenère • Hard

Vigenère with a 3-letter keyword. The plaintext mentions treasure:

```
DLC DVCKWSBI GC FSBMCN LCBI
```

Solver hint. Every third letter shares a shift. Guess that the message opens with THE; that alone reveals the 3-letter key.

A29. Telephone Keys

Logic & Patterns • Medium

On a phone keypad, letters map to digits (ABC=2, DEF=3, GHI=4, JKL=5, MNO=6, PQRS=7, TUV=8, WXYZ=9). Decode the digit string into one likely word:

```
4 3 5 5 6
```

Solver hint. Each digit covers 3–4 letters. Choose letters that spell a common word; 4-3-5-5-6 has a familiar greeting as a solution.

A30. Anagram Attack

Logic & Patterns • Easy

Unscramble this anagram of a word central to this competition:

```
HPCIRE
```

Solver hint. All six letters are used once. Think of words for a secret writing system.

A31. Classic Line

Caesar / Shift • Easy

Shift cipher. Decode:

```
EPP CSYV FEWI EVI FIPSRK XS YW
```

Solver hint. Test small shifts; the opening doubled letter narrows it quickly.

A32. Keyed Grid

Polybius Square • Hard

A Polybius square was filled starting with the keyword SECRET (then the rest of the alphabet, I/J merged) before numbering. Decode:

```
311234434511
```

Solver hint. First build the grid: write SECRET (dropping repeats → SECRT) then the remaining letters A,B,D,F,... Fill row by row, then read (row,column) pairs.

A33. Book Code

Logic & Patterns • Medium

Using the reference sentence `THE QUICK BROWN FOX`, each code pair is (word number, letter number within that word). Decode the pairs $(1,1)\,(2,2)\,(4,3)$:

Solver hint. First number selects the word, second selects the letter inside that word. Index carefully (counting from 1).

A34. Two Words

Encodings (A1Z26) • Easy

A=1..Z=26, hyphens within words:

`7-15 14-15-23`

Solver hint. Convert numbers to letters.

A35. Self-Reference

Logic & Patterns • Hard

How many letters are in the correct answer to this question, written as an English word? (The answer is a number word that equals its own letter count.)

Solver hint. Test small number words: does THREE have three letters? Does FOUR have four? Find the fixed point.

1.2 Round 2

A36. Red Planet

Vigenère • Medium

Vigenère, 4-letter keyword (a planet). Decode:

`FHV KQCFFP RFMZD ZK TAIVQR KZMN KZQ FZJET`

Solver hint. Key length 4: split into 4 columns, each a Caesar shift. The repeated THE pattern helps fix the key; the theme suggests a planet.

A37. Two Locks

Layered Ciphers • Hard

The plaintext was first Caesar-shifted by 3, then Atbash was applied. Peel both layers:

`TICVLS DFICVLS WPSWT`

Solver hint. Undo in reverse order: first reverse the Atbash (A↔Z), then shift back by 3.

A38. Five Columns — *Columnar Transposition • Hard*

Columnar transposition, keyword RIVER (5 columns), pad X. Decode:

`ROITXETERWRAHEAETVDXTTRAN`

Solver hint. Column read order follows alphabetical rank of R,I,V,E,R. Reconstruct rows = total/5, refill columns in that order, read across.

A39. The Long Game — *Monoalphabetic Substitution • Hard*

A longer substitution challenge:

`YPXMSKJKHXQCQ PONTCPOQ MKSCOJYO KJB MPKYSCYO`

Solver hint. With more text, frequency analysis is reliable. Lock E and T first, then use common digrams (TH, ER, IN) and the word THE to crack the rest.

A40. Philosopher's Key — *Vigenère • Hard*

Vigenère; the keyword is the surname of a philosopher associated with this very quote. Decode:

`LNQKYFDIS VUSGZS JS RCJFR`

Solver hint. The quote is attributed to Francis Bacon. Try BACON as the key, then verify it produces readable text.

A41. Anagram Hunt — *Logic & Patterns • Medium*

Unscramble the six letters `T,R,A,C,E,S` into a common English word meaning faint marks left behind:

Solver hint. All six letters are used exactly once. One natural answer means 'faint marks left behind'.

A42. Seven and Three — *Affine • Hard*

Affine cipher $E(x) = (7x + 3) \bmod 26$. Decode:

`JDGAFJDGHRZ HZ KFDNGHMNC`

Solver hint. Find $7^{-1} \bmod 26 = 15$. Then $D(y) = 15(y - 3) \bmod 26$ with A=0.

A43. Four Rails

Transposition (Rail Fence) • Hard

A 4-rail rail fence. Decode:

`TAIEHNLESDNLEICUHDWLFLIE`

Solver hint. Map the zigzag pattern for the known length over 4 rails, count letters per rail, deal back, and read along the zigzag.

A44. Modular Clock

Number Patterns • Hard

On a 12-hour clock, what time is it 100 hours after 7:00? Show the modular reasoning.

Solver hint. Add the hours and reduce modulo 12. This is the same arithmetic that powers shift ciphers (mod 26).

A45. Repeats Betray

Vigenère (Kasiski) • Hard

This Vigenère ciphertext repeats a phrase. Use the spacing of repeated groups to find the key length, then solve:

`LBR JUVF CA KJNAH GZY ESCA AH FHUVF`

Solver hint. Identical plaintext repeated at a distance that is a multiple of the key length yields identical ciphertext. Measure the gap between repeats; its divisors give candidate key lengths (here 3).

A46. Pigpen Preview

Logic & Patterns • Medium

In the Pigpen cipher, the first nine letters A–I sit in a 3×3 grid (A top-left, B top-middle, C top-right, ... I bottom-right), and each letter's symbol is the set of grid lines bordering its cell. Describe the symbol for the letter `E` (the centre cell).

Solver hint. Draw the 3×3 grid and look at how many sides enclose each cell. The centre is enclosed on every side.

A47. Maxim

Monoalphabetic Substitution • Hard

Decode this security maxim:

`SECUQFTY TDQNUBD NASCUQFTY FS MNT SECUQFTY`

Solver hint. A repeated long word (here the first and last) anchors several letters at once. Combine with E/T frequencies.

A48. Numbers Then Words

Layered Encodings • Medium

Decode A=1..Z=26 ('/' separates words):

`20 8 5 / 5 14 4`

Solver hint. Convert numbers to letters per word.

A49. Good Advice

Vigenère • Hard

Vigenère, 5-letter keyword (a financial review). Decode:

`AFZIRS WKMVK SRCK WIUS MWCFM`

Solver hint. Key length 5. Theme hints at AUDIT. Split into 5 Caesar streams and verify.

A50. Find the Rule

Logic & Patterns • Hard

A made-up operation # follows one consistent rule:

$3 \# 5 = 16, \quad 4 \# 6 = 25, \quad 5 \# 7 = ?$

Solver hint. Test a multiply-then-adjust rule against BOTH given equations before predicting the third.

A51. Wrapped Twice

Layered Ciphers • Hard

Plaintext was Caesar-shifted by 10, then Atbash applied. Decode:

`FLLA WIHX XLNYLW XPKL`

Solver hint. Reverse Atbash first, then shift back by 10.

A52. Night School

Columnar Transposition • Hard

Columnar transposition, keyword NIGHT, pad X. Decode:

`EETHXTHHOXEBDCXMENSLMIEOX`

Solver hint. Rank N,I,G,H,T alphabetically to get the column read order (G,H,I,N,T = 3,4,2,1,5). Rebuild and read across.

A53. Collatz Step

Number Patterns • Hard

Apply the rule: if even, halve; if odd, triple and add one. Starting at 6, list the next 4 values.

Solver hint. Check parity at each step and apply the matching operation.

A54. Repetition Pays

Vigenère • Hard

Vigenère, 5-letter keyword (what practice builds). Decode:

`HBINEAMM XLCOA APJPMNE AXLPPV`

Solver hint. Theme word SKILL has a repeated letter—useful when checking your key against the streams.

A55. Letter Math

Logic & Patterns • Medium

If `CAB` $= 3 + 1 + 2 = 6$ (A=1,...,Z=26), what does `FACE` equal?

Solver hint. Replace each letter by its alphabet position and add the four numbers.

A56. Weak Links

Monoalphabetic Substitution • Hard

Decode:

`TCS WSDISRT JGLI EQSDIR TCS FCDGL`

Solver hint. Anchor THE (appears twice). Then use common endings and the digram TH to expand.

A57. Column Read

Logic & Patterns • Hard

A word (padded with a trailing X) was written into a grid of 2 columns, one row at a time, then read column by column to give:

`HLOELX`

Recover the original 5-letter word.

Solver hint. The first half of the ciphertext is column 1 (top to bottom); the second half is column 2. Interleave them and drop the padding X.

A58. Eleven

Affine • Hard

Affine $E(x) = (11x + 4) \bmod 26$. Decode:

`WRAJINFOCR NJCFWAFU NJOBEAI`

Solver hint. $11^{-1} \bmod 26 = 19$. Then $D(y) = 19(y - 4) \bmod 26$.

A59. Mightier *Vigenère • Hard*

Vigenère, 3-letter keyword (what a pen holds). Decode:

`BUO XRX QF WQTRBVOZ GRIA DPR CEBBL`

Solver hint. Key length 3; opening THE fixes the key immediately.

A60. Letter Hunt *Logic & Patterns • Hard*

Take the 3rd letter of `CRYPTO`, the 1st letter of `OLYMPIAD`, and the 2nd letter of `ISLAMABAD`. Reorder the three letters into a common English word.

Solver hint. Extract each indexed letter (counting from 1), then find the three-letter word they form.

A61. One Word *Morse Code • Easy*

Decode:

`.- .. -.`

Solver hint. E/T are single symbols; build out.

A62. Almost There *Caesar / Shift • Medium*

Shift cipher. Decode:

`QDXOJMT DN IZVM FZZK BJDIB`

Solver hint. A large shift is the same as a small backward shift; try shifting forward by 5.

A63. The Door *Vigenère • Hard*

Vigenère, 4-letter keyword (an entrance). Decode:

`ZHX PGSM TAZSPK OIITS MLK DHSX`

Solver hint. Theme suggests GATE; verify with the THE anchor.

A64. Parity Check

Logic & Patterns • Medium

A 7-bit code carries 6 data bits plus 1 parity bit chosen so the total number of 1s is even. Is `1011010` valid under even parity?

Solver hint. Just count the 1 bits; even parity requires an even count.

A65. Index of Coincidence (concept)

Logic & Patterns • Hard

Two ciphertexts are given. One is a simple substitution of English; the other is random letters. Without decrypting, how can letter-frequency shape tell them apart?

Solver hint. Substitution only renames letters—it cannot flatten their uneven counts. Compare how uneven each frequency distribution is.

2 Professional Track (Open)

2.1 Round 1

P01. Textbook RSA

RSA • Medium

Given RSA public key ($n = 3233,\ e = 17$) with primes $p = 61, q = 53$, and ciphertext $c = 2790$, recover the message m (an integer).

Solver hint. You know the factorization, so compute $\phi(n) = (p-1)(q-1)$, invert e modulo ϕ to get the private exponent d, then exponentiate the ciphertext.

P02. Factor First

RSA • Medium

An RSA modulus $n = 11413$ is small enough to factor by hand. With $e = 11$ and ciphertext $c = 4447$, find m.

Solver hint. Trial-divide n by small primes to find p, q (try values near $\sqrt{n}$). Then proceed as standard RSA decryption.

P05. Shared Secret

Diffie–Hellman • Medium

In Diffie–Hellman with prime $p = 23$ and generator $g = 5$, Alice sends $A = 8$ and Bob sends $B = 19$. Eve also learns Alice's secret $a = 6$. What shared secret s do they compute?

Solver hint. The shared secret is $B^a \bmod p$ (equivalently $A^b \bmod p$). You are given a, so use the first form.

P07. Three Properties

Hash Functions • Medium

Name the three core security properties expected of a cryptographic hash function, and give a one-line meaning of each.

Solver hint. Two of the properties fix one input and search for a matching one; the third fixes nothing and just seeks any colliding pair.

P08. Birthday Bound

Hash Functions • Medium

A hash outputs 128-bit digests. Roughly how many random inputs must you try before a collision becomes likely, and which attack does this describe?

Solver hint. Collisions appear far sooner than 2^n; the relevant scale is the square root of the output space.

P10. ECB Penguin

Block Cipher Modes • Medium

Why does encrypting an image with AES in ECB mode still leak the image's outline, while CBC does not?

Solver hint. Ask what ECB does with two identical input blocks, and how CBC's chaining/IV breaks that.

P11. IV Basics

Block Cipher Modes • Medium

In CBC mode, what are the two essential requirements on the initialization vector (IV), and what breaks if each is violated?

Solver hint. Think separately about predictability (before encryption) and uniqueness (across messages).

P12. Single-Byte XOR

XOR / OTP • Easy

A two-byte message was XORed with a single repeated key byte, giving ciphertext (hex) `6263`. The key byte is `0x2A`. Recover the ASCII text.

Solver hint. XOR is its own inverse: re-XOR each ciphertext byte with the key byte to get the original ASCII codes.

P14. Kerckhoffs's Principle

Principles • Easy

State Kerckhoffs's principle and explain why "security through obscurity" of the algorithm is discouraged.

Solver hint. The principle isolates exactly one secret. Consider what happens to a secret algorithm once it leaks versus what happens when only a key leaks.

P20. Little Theorem

Number Theory • Medium

Using Fermat's Little Theorem, compute $3^{100} \bmod 7$ without a calculator.

Solver hint. Fermat gives $a^{p-1} \equiv 1 \pmod{p}$. Reduce the exponent modulo $p - 1 = 6$ first.

P21. Password Entropy

Key Management • Medium

A password is 8 characters chosen uniformly from a 95-character printable set. Estimate its entropy in bits and state whether it resists offline brute force today.

Solver hint. Entropy = length $\times \log_2$(alphabet size). Compare the result to the $\sim 2^{60+}$ guesses attackers can make offline.

P22. Encrypt vs Authenticate

Integrity • Medium

Encryption alone (e.g. AES-CBC) does not guarantee integrity. Give a concrete example of tampering it fails to stop, and name the property/primitive that fixes it.

Solver hint. Confidentiality $\neq$ integrity. Think about whether the receiver can tell the ciphertext was modified, and which primitive certifies authenticity.

P24. Applied Frequency

Cryptanalysis • Medium

Break this monoalphabetic substitution (long enough for statistics):

`QAT CPUCIYTP MJSIP NTKCMCQTN QAT KMTKCMTP OMJF QAT MTNQ`

Solver hint. Lock the highest-frequency ciphertext letter to E and the most common three-letter word to THE. Then exploit digrams (TH, ER) and the repeated word THE to finish.

P26. Why Salt

Password Storage • Medium

Why are password hashes salted, and what additional defense does a slow hash (bcrypt/Argon2) add on top of salting?

Solver hint. Salt addresses precomputation and duplicate detection; slowness addresses the raw guessing rate. They solve different problems.

P27. Modular Inverse

Number Theory • Medium

Find $17^{-1} \bmod 43$ using the extended Euclidean algorithm.

Solver hint. Run the extended Euclidean algorithm on $(17, 43)$ to write $1 = 17x + 43y$; then $x \bmod 43$ is the inverse.

2.2 Round 2

P03. Cube Root — *RSA • Hard*

A message m was encrypted with $e = 3$ and a modulus so large that $m^3 < n$ (no wraparound occurred). The ciphertext is $c = 64$. Recover m.

Solver hint. If $m^3 < n$ then $c = m^3$ exactly—no modulus involved. Just take the real cube root of c.

P04. Why Pad? — *RSA / Signatures • Hard*

Plain "textbook" RSA encryption ($c = m^e \bmod n$, no padding) is deterministic. Name TWO concrete weaknesses this causes for short or low-entropy messages, and name the standard fix.

Solver hint. Think about what 'deterministic' leaks when the message space is small, and what algebraic property m^e preserves under multiplication.

P06. Find the Exponent — *Discrete Log • Hard*

Solve the discrete logarithm: find x with $2^x \equiv 22 \pmod{29}$, $0 < x < 29$.

Solver hint. Brute force is feasible here: build a table of $2^1, 2^2, 2^3, \ldots \pmod{29}$ until you hit the target.

P09. Length Extension — *Hash Functions • Hard*

Why is MAC $= H(\text{secret} \,\|\, \text{message})$ insecure for Merkle–Damgård hashes like SHA-256, and what standard construction fixes it?

Solver hint. Merkle–Damgård hashes expose the internal state as the output, letting an attacker continue hashing. The fix wraps the hash in a keyed, nested structure.

P13. Two-Time Pad — *XOR / OTP • Hard*

Two messages were encrypted with the SAME one-time-pad key (a 'two-time pad'). An eavesdropper computes $C_1 \oplus C_2$. What does this equal, and why does it break confidentiality?

Solver hint. Write each ciphertext as plaintext XOR key and XOR the two together; watch the key terms cancel.

P15. Padding Oracle

Attacks • Hard

In CBC mode with PKCS#7 padding, an attacker can decrypt ciphertext without the key if the server reveals whether padding is valid. In one or two sentences, what information does each query leak, and why is that enough?

Solver hint. Focus on the single yes/no the oracle returns and how altering the preceding block's bytes turns that bit into knowledge of the intermediate state.

P16. Nonce Reuse

Stream Ciphers • Hard

A stream cipher generates keystream from (key, nonce). What goes catastrophically wrong if the same (key, nonce) pair encrypts two different messages?

Solver hint. Keystream depends only on (key, nonce). If that pair repeats, the keystream repeats—connect this to the two-time-pad problem.

P17. Matrix Key

Hill Cipher • Hard

A 2×2 Hill cipher uses key $K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$ over $\mathbb{Z}_{26}$ (A=0). The ciphertext digraph is `HI`. Recover the plaintext pair.

Solver hint. Compute the determinant mod 26 and its modular inverse, build K^{-1} mod 26 via the adjugate, then multiply by the ciphertext vector.

P18. Recover the Key

Known-Plaintext • Hard

An affine cipher maps plaintext A→F and B→K. Determine the affine key (a, b) in $E(x) = (ax + b) \bmod 26$.

Solver hint. Plug the two known pairs into $E(x) = ax + b$. The first gives b directly; the second then gives a.

P19. Chinese Remainder

Number Theory (CRT) • Hard

Find the smallest positive x with $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

Solver hint. Combine two congruences at a time, or use the Chinese Remainder Theorem with moduli product 105.

P23. Why ECC

Elliptic Curves • Hard

ECC offers equivalent security to RSA at much smaller key sizes (e.g. 256-bit ECC ≈ 3072-bit RSA). What underlying hard problem does ECC rely on, and why does it scale better than RSA's?

Solver hint. Compare the best-known attack complexities: factorization has a sub-exponential method, whereas the elliptic-curve discrete log does not.

P25. Forward Secrecy

Protocols (TLS) • Hard

What is forward secrecy, and which key-exchange choice provides it in TLS versus which does not?

Solver hint. Ask whether compromising the server's long-term key tomorrow should expose traffic recorded today. The answer hinges on ephemeral vs static key exchange.

P28. Broadcast Attack

RSA • Hard

The same message m is sent to three people with $e = 3$ and three different moduli n_1, n_2, n_3 (pairwise coprime), giving c_1, c_2, c_3. How can an attacker recover m without factoring any modulus?

Solver hint. Combine the three ciphertexts with the Chinese Remainder Theorem to learn m^3 modulo the product, then note m^3 is smaller than that product.

P29. GCM Nonce Reuse

AEAD • Hard

AES-GCM is a popular AEAD mode. What two distinct security guarantees does it provide, and what specifically breaks if a (key, nonce) pair is ever reused?

Solver hint. GCM is CTR encryption plus a polynomial MAC. Consider what nonce reuse does to the CTR keystream and, separately, to the authentication tag's secrecy.

P30. Timing Leak

Side Channels • Hard

A string-comparison function for checking MACs returns as soon as it finds a mismatched byte. Why is this dangerous, and what is the fix?

Solver hint. The leak is in *how long* the check takes, not its yes/no result. Remove the data-dependence in the comparison's running time.