Answers to Exercises

1.1

1. ZMW ZUGVI GSVN GSV PRMT LU HSVHSZXS HSZOO WIRMP
2. THIS WHOLE LAND SHALL BECOME A RUIN AND A WASTE
3. JUST AS WATER REFLECTS THE FACE, SO ONE HUMAN HEART REFLECTS ANOTHER.
4. EDUCATION ISANORNAM ENTINPROS PERITYAND AREFUGEIN ADVERSITY
5. THE SCYTALE WAS AN EARLY EXAMPLE OF A TRANSPOSITION CIPHER
6. (a) IULHQGV URPDQV FRXQWUBPHQ OHQG PH BRXU HDUV
   (b) BEWARE THE IDES OF MARCH
   (c) PNA JR RIRE UNIR GBB ZHPU BS N TBBQ GUVAT
   (d) BEING ISBET TERTH ANSEE MINGT OBE
7. I k m c & m i c l T z v v g x g z t h A f m a n e o k o L x & q f k c y d I a k
8. ALBERTI WROTE ON PERSPECTIVE IN 1434
9. XWLEXV IRLPMON ISZVTY LHPBCEQ HH SRTRLNQ IWFA MMQVZKC
10. GALILEO GALILEI OBSERVES PENDULUM PERIODS
11. YOU BROKE IT
12. BACON SAID IT X
13. (a) KNOWLEDGE IS MORE THAN EQUIVALENT TO FORCE

(b) NO ONE BUT A BLOCKHEAD EVERY WROTE EXCEPT FOR MONEY

14. WELL-GOT WEALTH MAY MEET DISASTER, BUT ILL-GOT WEALTH DESTROYS ITS MASTER.

15. This would implement a simple shift cipher. Once the shift amount was discovered by a cryptanalyst, the message would be easily obtained.

16. UG FB JH KV FD UX OC PG HA JE OH NB PC FJ YG XM DF GJ

17. WE ARE NOT INTERESTED IN THE POSSIBILITES OF DEFEAT

18. WASHINGTON, DC. JULY 15, 1863. FOR SIMON CAMERON. I WOULD GIVE MUCH TO BE RELIEVED OF THE IMPRESSION THAT MEADE, COUCH, SMITH AND ALL, SINCE THE BATTLE OF GETTYSBURG HAVE STRIVEN ONLY TO GET THE ENEMY OVER THE RIVER WITHOUT ANOTHER FIGHT. PLEASE TELL ME IF YOU KNOW WHO WAS THE ONE CORPS COMMANDER WHO WAS FOR FIGHTING, IN THE COUNCIL OF WAR ON SUNDAY NIGHT. SIGNED A. LINCOLN

19. AFGVFF GFVAAG VAXGVG AVXDXX VVAXVA GVGDGG

20. ENEMY RETREATING

21. BETWEEN FRIENDS THERE IS NO NEED OF JUSTICE

22. (a) Blocks of b letters are rotated r letters to the right.

    (b) THE UNIVERSE IS MADE OF STORIES, NOT ATOMS.

    (c) GIVE THE PEOPLE A NEW WORD AND THEY THINK THEY KNOW A NEW FACT.

    (d) SECRECY IS THE FIRST ESSENTIAL IN AFFAIRS OF THE STATE.

23. (a) When the sum of the digits is divided by 10, the remainder is 5, so there is a digit in error.

    (b) Let $d_1\,d_2\,d_3\,d_4\,d_5 \quad d_6\,d_7\,d_8\,d_9 \quad d_{10}\,d_{11} \quad c$ be the correct digits of the postal address code. If a scan of this code is uncertain only in digit 1, then the scanner computes the checksum $\tilde{d}_1 + d_2 + d_3 + d_4 + d_5 + d_6 + d_7 + d_8 + d_9 + d_{10} + d_{11} + c$ and determines the remainder when this number is divided by 10. If the remainder is 0, then $\tilde{d}_1 = d_1$, and if the sum is not 0, then $\tilde{d}_1 \neq d_1$.

    (c) The postal address code 14850 1000 30 8 is correct, and so is 15840 1000 30 8.

24. (a) $M = 1033$, $e = 11410$, $d = 5187$, and $n = 57293$.
    (b) The enciphered PIN is 53803.
    (c) $d = 52135$, PIN = 2000

1.2

1. (a) $f(\texttt{A}) = \texttt{M}$, $f(\texttt{V}) = \texttt{R}$

(c)

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$f^{-1}(x)$	G	M	N	O	L	P	Q	I	B	R	S	K	A
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$f^{-1}(x)$	T	J	F	U	V	W	D	E	X	H	C	Y	Z

2. ATHEMATICSMAY ISAY ETHAY ANGUAGELAY OFAY ECRETSAY ITINGWRAY

3. If x is the numerical plaintext, then the ciphertext is $y = 25 - x$. Applying this twice gives $25-(25-x) = x$, so Atbash is an involution.

4. (a) $e(e(e(e(\texttt{AMAZING})))) = \texttt{AMAZING}$
   (b) For any letter except M or N, four applications of e returns that letter. Two applications of e to either M or N returns the letter, and since 2 divides 4, e returns any single letter and therefore any string after four applications.
   (c) After applying e once to a string x, three more applications return the string. Thus the inverse of e is three applications of e; $d(x) = e(e(e(x)))$.

5. The composition is also a simple substitution.

6. (a) $P(s(\texttt{ARITHMETIC})) = P(\texttt{RATIMHTECI}) = 42114424322344151324$, but $s(P(\texttt{ARTHMETIC})) = s(11422444233315442313) = 11244244323351443213$, so in general $P(s(x)) \neq s(P(x))$.

2.1

1. (a) ELVIS WAS SIGHTED AT MAIN AND UNION
   (b) PRESIDENT AND CONGRESS REACH BUDGET AGREEMENT

2. (b) Shift by 10 and then by 16 to achieve a net shift of 26, which is zero modulo 26.

3. (a) $127 = (18)7 + 1$, (b) $473 = (18)26 + 5$, (c) $1024 = (64)16 + 0$, (d) $3 = (0)14 + 3$, (e) $-43 = (-11)4 + 1$, (f) $-123 = (-1)124 + 1$

4. (a) 2, (b) 0, (c) 4, (d) 14

5. (a)

x	0	1	2	3	4	5	6	7
$(x+2)$ MOD 8	2	3	4	5	6	7	0	1

(b)

x	0	1	2	3	4	5	6	7	8	9	10
$(x+2)$ MOD 11	2	3	4	5	6	7	8	9	10	0	1

(c)

x	0	1	2	3	4	5	6	7	8	9
$(x+5)$ MOD 10	5	6	7	8	9	0	1	2	3	4

(d)

x	0	1	2	3	4	5	6	7	8	$\cdots$	22	23
$(x-6)$ MOD 24	18	19	20	21	22	23	0	1	2	$\cdots$	16	17

(e)

x	0	1	2	3	4	5	6	7	8	9	10	11
$(x+2)$ MOD 11	1	2	3	4	5	6	7	8	9	10	11	0

6. (a) 9, 35, 61, 87, 113, 139; (b) 2, 6, 10, 14, 18, 22

7. (a) 5; (b) -7 (c) 3; (d) 1; (e) 5; (f) 320019755

8. $a \equiv b \pmod m$ means that $a = b + km$ for some integer k. Now the number $r = b$ MOD m satisfies $b = qm + r$, where $0 \le r < m$, so $a = qm + km + r = (q + k)m + r$. This says that $a \equiv r \pmod m$, that is, $a \equiv b$ MOD $m \pmod m$. The same reasoning shows that $b \equiv a$ MOD $m \pmod m$.

9. `AOLMB SSULZ ZVMSP MLPZP UAOLO HGHYK ZVMSP ML`

10. Let $y = x + 11 \pmod{26}$;

    `POFNLETZY TD ESP MPDE ACZGTDTZY QZC ZWO LRP`

11. `IF YOU CAN'T BE KIND, AT LEAST BE VAGUE`

12. The deciphering formula is $x = y - 18 \pmod{26}$ or $x = y + 8 \pmod{26}$.
    `WHEN YOU COME TO A FORK IN THE ROAD TAKE IT`

13. `TRUE WORTH IS IN BEING NOT SEEMING`

14. `FOLLOWYOURBLISS`

15. `PROSPERITY IS NOT WITHOUT MANY FEARS AND DISTATES, AND ADVERSITY IS NOT WITHOUT COMFORTS AND HOPES.`

2.2

1. Multiplication modulo 8 is, e.g.

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

   The numbers having no factor (other that 1) in common with 8 have an inverse.

2. (a) 17; (b) 5; (c) 5; (d) 59

3. (a) 4; (b) 4; (c) 2; (d) 3; (e) 7; (f) 24;

4. $a = 19$, $b = 13$; (b) $a = 14$, $b = 5$

5. (a) $x = 17(y - 10) \mod 26$
   (b) $x = 5(y - 5) \mod 13$
   (c) $x = 5(y - 8) \mod 9$
   (d) $x = 59(y - 30) \mod 60$

6. (a)

x	1	3	7	9
$x^{-1} \pmod{10}$	1	7	3	9

   (b)

x	1	2	3	4	5	6	7	8	9	10
$x^{-1} \pmod{11}$	1	6	4	3	9	2	8	7	5	10

   (c)

x	1	5	7	11	13	17	19	23
$x^{-1} \pmod{24}$	1	5	7	11	13	17	19	23

7. `ZLZGB GZROZ DGWND ZOHNA NDGQ RALRQ QIBGG`

8. `IMAGINATION IS MORE IMPORTANT THAN KNOWLEDGE`

9. $a = 11$, $b = 6$. Plaintext: `IF YOU BOW AT ALL BOW LOW`

10. PROSPERITY IS NOT WITHOUT MANY FEARS AND DISTATES AND ADVERSITY IS NOT WITHOUT COMFORTS AND HOPES.

11. $a = 39x$, $q = 34x$

12. (a) An affine cipher is of the form $y \equiv ax + b$. There are 12 possible values for a that have multiplicative inverses and 26 possible values for b. Thus there are $12 \cdot 26 = 312$ different affine ciphers. For the choice $a = 1$ and $b = 0$, the cipher does nothing. So there are $312 - 1 = 311$ nontrivial affine ciphers on a 26-letter alphabet.

    (b) There are 28 choices for a and 29 choices for b, so there are $28 \cdot 29 = 812$ possible affine ciphers; only 811 of these are nontrivial.

13. Note that $(n-1) \cdot (n-1) \equiv n^2 - 2n + 1 \equiv 0 - 0 + 1 \equiv 1 \pmod{n}$.

14. Suppose that $a^2 \equiv 1 \pmod{p}$. Then p divides $a^2 - 1 = (a-1)(a+1)$. Since $a > 1$ and $a < p - 1$, the factors are nontrivial; since p is prime, p must divide either $a - 1$ or $a + 1$, both of which are less than p and positive. This is impossible, so there is no a in the range 2 to $p - 2$ such that $a^{-1} \equiv a \pmod{p}$.

2.3

1. (a) ABCDEFGHIJKLMNOPQRSTUVWXYZ
    NATURLSECIOBDFGHJKMPQVWXYZ
    Ciphertext: C ENVR TNBRU PECM HKCFTCHBR AY WECTE RNTE MBCDEP VNKCNPCGF CL MRLOB CM HKRMRKVRU FNPQKNB MRBRTPCGF

    (b) WE WILL NOW DISCUSS IN A LITTLE MORE DETAIL THE STRUGGLE FOR EXISTENCE.

2. (a)
plain	ABCDEFGHIJKLMNOPQRSTUVWXYZ
cipher	PAKYRBLZICOMDQEFUNGVSHWTJX

    (b) IVIGD SKZRP GIRNV EARKN IVIKP MVZPQ VEARK ENNRK V

    (c) APREC EDENT EMBAL MSAPR INCIP LE

3. (a) THREE MAY KEEP A SECRET IF TWO OF THEM ARE DEAD.

    (b) EDUCATION HAS BECOME A PRISONER OF CONTEMPORANEITY. IT IS THE PAST, NOT THE DIZZY PRESENT, THAT IS THE BEST DOOR TO THE FUTURE.

(c) WE MUST ALL HANG TOGETHER OR ASSUREDLY WE SHALL ALL HANG SEPARATELY.

(d) I'D RATHER BE A LIGHTNING ROD THAN A SEISMOGRAPH.

(e) LIFE IS ALWAYS A RICH AND STEADY TIME WHEN YOU ARE WAITING FOR SOMETHING TO HAPPEN OR HATCH.

(f) THE TRUTH IS ALWAYS SOMETHING THAT IS TOLD, NOT SOMETHING THAT IS KNOWN. IF THERE WERE NO SPEAKING OR WRITING, THERE WOULD BE NO TRUTH ABOUT ANYTHING. THERE WOULD ONLY BE WHAT IS.

4. FOURSCORE AND SEVEN YEARS AGO OUR FATHERS BROUGHT FORTH ON THIS CONTINENT A NEW NATION CONCEIVED IN LIBERTY AND DEDICATED TO THE PROPOSITION THAT ALL MEN ARE CREATED EQUAL,

   keyword LINCOLN

plain	ABCDEFGHIJKLMNOPQRSTUVWXYZ
cipher	LAGPUZIBHQVNDJRWCEKSXOFMTY

5. I KNOW NOT WHAT COURSE OTHERS MAY TAKE; BUT AS FOR ME, GIVE ME LIBERTY OR GIVE ME DEATH.

6. THE FACT THAT THERE ARE IRRATIONAL NUMBERS THAT ARE NOT FRACTIONS CAME AS A GREAT SURPRISE TO THE GREEKS AND IS STILL PROBABLY UNFAMILIAR TO MOST OF THE WORLDS INHABITANTS

7. A SHORT SAYING OFT CONTAINS MUCH WISDOM

10. $26! = 403291461126605635584000000 \equiv 4.03 \times 10^{26}$, so the time is $4.03 \times 10^{26}/19^9$ sec $= 4.03 \times 10^{17}$ sec $= 1.28 \times 10^{10}$ years.

2.4

1. EUCLID ALONE HAS LOOKED ON BEAUTY BARE.

2. WELL, IF I CALLED THE WRONG NUMBER, WHY DID YOU ANSWER THE PHONE?

3. ITWMA ONAW ITEOH FADKH AMRST ONNHS RITSO NIKAE EIKOG EENNH TNOCE NCRVN TOPNO GETOW HSMOV EOHFR TTOPT

4. CEHIT OTDRC EESDS TDUMN LESCH LETOI SIOO ENIAE LHMEE RCTWR AVHWP TMSBT DIEOM NTSPI ONESE DHFYO DIUWN STBMI RVINT LII

5. GIVE ME SOMEWHERE TO STAND AND I WILL MOVE THE EARTH.

6. MATHEMATICS MAY BE DEFINED AS THE SUBJECT WHERE WE NEVER KNOW WHAT WE ARE TALKING ABOUT NOR WHETHER WHAT WE ARE SAYING IS TRUE.

7. (a) 8, 7, 6, 4, 1, 8

   (b)

x	1	2	3	4	5	6	7	8	9	10
$p^{-1}(x)$	4	3	6	1	10	2	9	5	7	8

   (c) NEVER HELP A CHILD WITH A TASK AT WHICH HE FEELS HE CAN SUCCEED.

2.5

1. (a) RSJVE SAVBV OKNFC IEIZT ICRRU XRFCR ESIIN IJKS

   (b) DEYIE GATIC VBKT KBDRN AJEXU IQLRY IRPZT HKYUW

2. (a) MATHEMATICS IS ONLY THE ART OF SAYING THE SAME THING IN DIFFERENT WORDS.

   (b) THERE IS NO OTHER ROYAL PATH WHICH LEADS TO GEOMETRY.

3. (a) PXTVMSUC

   (b) QLBLESGA

   (c) EYNUZCUB

   (d) QLTWVWUP

4. BEAUTY IS ONLY THE PROMISE OF HAPPINESS

5. THE TRUTH IS ALWAYS SOMETHING THAT IS TOLD, NOT SOMETHING THAT IS KNOWN. IF THERE WERE NO SPEAKING OR WRITING, THERE WOULD BE NO TRUTH ABOUT ANYTHING. THERE WOULD ONLY BE WHAT IS.

6. (i) is the polyalphabetic substitution; (ii) is the transposition; (iii) is the monoalphabetic substitution

9. (b) WHEN WE ARE CHAFED AND FRETTED BY SMALL CARES, A LOOK AT THE STARS WILL SHOW US THE LITTLENESS OF OUR OWN INTERESTS.

2.6

1. $P(6, 3) = 120$, $P(5, 5) = 120$, $P(10, 2) = 90$, $P(26, 4) = 358\,800$, $P(365, 4) = 1.74586 \times 10^{10}$
2. $C(6, 3) = 20, C(5, 5) = 1, C(10, 2) = 45, C(26, 4) - 14\,950, C(365, 4) = 727\,441\,715$
3.

							1		6		15		20		15		6		1								
					1		7		21		35		35		21		7		1								
			1		8		28		56		70		56		28		8		1								
		1		9		36		84		126		126		84		36		9		1							
	1		10		45		120		210		252		210		120		45		10		1						

   $C(8, 8) = 1$, $C(9, 4) = 95$, $C(10, 3) = 120$
4. number of 3-letter words $= P(7, 3) = 210$, $P(7, 5) = 2520$, $C(7, 3) = 35$, $C(7, 5) = 21$
5. (a) $P(15, 10) = 1.089729 \times 10^{10}$
   (b) $P(8, 4) = 1680$
6. (a) $C(15, 10)3003$; (b) $C(8, 4) = 70$
7. (a) 17 576 000 (b) 200, 1000 (c) 5.680024×10^{10}
8. (a) 1/6 (b) 1/2 (c) 1/3 (d) 5/6 (e) 2/3
9. (a) 1/36 (b) 1/18 (c) 1/12 (d) 11/12 (e) 5/18
10. (a) 0 (b) 0.105 (c) 1 (d) 0.362 (e) 0.683 (f) 0.578
11. (a) 0.066 (b) 0.011 (c) .081469 (d) 0.1631 (e) 0.897 (f) 0.28
12. (a) 239, 410 (b) 74, 57, 6, 168
13. (a) about 5 (b) 0.00148, about 15
14.

n	1	2	$\cdots$	6	7	8	9	10	11	12
$b(n)$	0	0.032	$\cdots$	0.383	0.5023	0.615	0.714	0.797	0.863	0.911

   where $b(n)$ is the probability of at least 1 pair of coincident birthdays in a group of n people with birthdays in May. Thus, to be at least 50% certain of at least 1 pair of coincident birthdays, 7 people must be 90% certain, 12 people must be selected.
15. (a) 0.0745, 0.106, 0.35
    (b) 0.0023, 0.00183

2.7

1. (a) $7.07005 \approx 7$
   (b) $1.99094 \approx 2$
   (c) $1.17222 \approx 1$
   (d) $1.0076 \approx 1$, suggests a monoalphabetic substitution

2. The index of coincidence is 0.040 and the estimated keyword length is 19. This differs significantly from the keyword length estimates of 2, 4, or 8 obtained by the Kasiski test. However, since this is a fairly large number, it strengthens the hypothesis that the keyword length is 8.

3. The index of coincidence is: .071 and the keyword length is: $.813 \approx 1$. On the basis of the Friedman test alone, we would conjecture that this is a monoalphabetic substitution.

4. If $I = .03850001$. the keyword length estimate is

   $$k \approx 0.0265n/(.026499 + .0000001n).$$

   If n is large, on the order of 10 000, then this number is about 9 636. In general, if the index of coincidence is close to 0.0385, the estimated keyword length is about n, the length of the message itself.

   If $I = .06499$ then the estimate of the keyword length is

   $$0.0265n/(0.00001 + .02649n).$$

   For n large, say on the order of 10 000, this gives $k \approx 1$. In general, if the index of coincidence is near 0.065, the ciphertext is likely to be the result of a monoalphabetic substitution.

6. `HOPE IS DEFINITELY NOT THE SAME THING AS OPTIMISM. IT IS NOT THE CONVICTION THAT SOMETHING WILL TURN OUT WELL, BUT THE CERTAINTY THAT SOMETHING MAKES SENSE, REGARDLESS OF HOW IT TURNS OUT.`
   Keyword is `PEACE`.

7. (a) A 1100-letter sample of French gives an s value of 0.0889644
   (b) Using the given keyword estimation formula, we obtain $k \approx (0.0889644 - 0.0385) \cdot 523/((0.0889644 - 0.0531) + 523 \cdot (0.0531 - 0.0385)) = 3.43393 \approx 3$.

8. The keyword length is 6. Indeed, the keyword is in the footnote to this quotation.

2.8

1. Keyword length is 4.
2. (b) is monoalphabetic; (a) is polyalphabetic with keyword length 3
3. (a) Plaintext in both cases is

```
Genius is no more than childhood recaptured at will,
childhood equipped now with mans physical means
to express itself, and with the analytical mind
that enables it to bring order into the sum of experience,
involuntarily amassed.
```

   (b) Keyword is `NOW`.

5. The keyword is `MATH`.
6. Keyword is `KING`. Plaintext is

```
When, in the course of human events, it becomes necessary
for one people to dissolve the political bands which
have connected them with another, and to assume among
the powers of the earth the separate and equal station
to which the laws of nature and of nature's God entitles
them, a decent respect to the opinions of mankind requires
that they should declare the causes which impel them
to the separation.
```

2.9

1. (a) $\begin{bmatrix} 5 & 5 \\ 5 & 3 \end{bmatrix}$ (b) $\begin{bmatrix} 4 & 4 \\ 8 & 8 \end{bmatrix}$ (c) $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ (d) $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$
   (e) $\begin{bmatrix} 22 & 14 \\ 8 & 4 \end{bmatrix}$ (f) $\begin{bmatrix} 23 & 22 \\ 20 & 8 \end{bmatrix}$ (g) $\begin{bmatrix} 8 & 3 \end{bmatrix}$
2. (a) $\begin{bmatrix} 0 & 0 \\ 3 & 6 \end{bmatrix}$; (b) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$; (c) $\begin{bmatrix} 13 & 0 \\ 0 & 13 \end{bmatrix}$; (d) $\begin{bmatrix} 18 \\ 10 \end{bmatrix}$
3. (a) 1, (b) 4, (c) 0, (d) 19, (e) 18, (f) 25

4. $(a)\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ $(b)\begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}$ (c) not invertible
   $(d)\begin{bmatrix} 12 & 9 \\ 1 & 6 \end{bmatrix}$ (e) not invertible $(f)\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
5. `OQZKLUVYDW`
6. `BONAPETITX`
7. (a) $A^{-1} = \begin{bmatrix} 9 & 10 \\ 10 & 9 \end{bmatrix}$; ciphertext = `IUWCWKPSYZ`.
   (b) `GO AHEAD`
8. `LUNCH IS ON ME.`
9. $A = \begin{bmatrix} 21 & 25 \\ 12 & 23 \end{bmatrix}$.
10. $A = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}$; $A^{-1} = \begin{bmatrix} 2 & 21 \\ 25 & 3 \end{bmatrix}$. `DEAR BOB, MARRY ME`
11. (a) is the Hill ciphertext; (b) is the monoalphabetic substitution.
12. Yes, the scheme is more secure. There is no other 2×2 Hill encipherment that will replicate the composition of the Hill and transposition ciphers. Also, there is no other transposition that will accomplish the substitution and transposition carried out by the composition.
13. 678-953-2900
14. (a) $A^{-1} = \begin{bmatrix} 1 & 2 & 2 \\ 3 & 3 & 0 \\ 0 & 3 & 3 \end{bmatrix}$.
    (b) $A^{-1} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 10 \end{bmatrix}$.
    (c) $A^{-1} = A$.
15. (a) `AAA YOC VWSHQG`.

(a) $A^{-1} = \begin{bmatrix} 1 & 2 & 20 \\ 25 & 25 & 4 \\ 0 & 25 & 3 \end{bmatrix}$; `ME COLD`.

16. If $\det(A)$ were not relatively prime to m, its multiplicative inverse would not be defined.

17. 16, 6.

18. 3^4 matrices and 42 of them invertible

19. If A_i is the ith row of A and B_j is the jth column of B then the ijth entry of AB is A_iB_j, so the ijth entry of $k(AB)$ is $k \cdot (A_iB_j)$. This, in turn, is equal to $(k \cdot A_i)B_j$, by the distributive law of arithmetic, and this last expression is the ijth entry of the matrix product $(kA)B$.

3.1

1. (a) 33, (b) 48, (c) 171, (d) 511,

2. (a) 1 000 000, (b) 10 000 001, (c) 11 101, (d) 100 011 111

3. (a) 17, (b) $\lceil \ln(10\,643\,522)/\ln 2 \rceil = 24$

4. 1 001 110, 1 001 111, 1 010 000, ...

5. `STAY CALM`

6. (a) 676, (b) 17 575, (c) 2398, (d) 1371, (e) 8 943 601

7. (a) `BB`, (b) `BAD`, (c) `CAAA`, (d) `CONE`, (e) `SPHERE`

8. (a) 4, (b) 6

9. `MEMPHIS`, `MEMPHIT`, `MEMPHIU`, `MEMPHIV`, `MEMPHIW`, `MEMPHIX`, `MEMPHIY`, `MEMPHIZ`, `MEMPHJA`, `MEMPHJB`, `MEMPHJC`, `MEMPHJD`, `MEMPHJE`, `MEMPHJF`, `MEMPHJG`, `MEMPHJH`

10. (a) 110 000, 110, (b) 101 111, 100001 (c) $a = 1\,110\,100$, $b = 10$
    (d) $a = 10\,000\,100$, $b = 1\,111\,010$

11. (a) $a + b =$`CPQ`, $a - b =$`OE`
    (b) $a + b =$`HOUHA`, $a - b =$`HOPDI`

(c) $a + b =$OUT, $a - b =$IN

12. $a =$MJD, $b =$LVP

13. (a) TWUTH MBHSE VTQCW

    (b) LOOSE LIPS SINK SHIPS[1]

14. THE PHILOSOPHER SPEAKS

15. The number of base twenty-six digits in n is $\lfloor \log_{26}(n) \rfloor + 1 = \lfloor \ln(n)/\ln(26) \rfloor + 1$. So the number of base twenty-six digits in 1234567890 is 7.

3.2

1. (a) $((1 + x_1)(1 + x_2) + x_1x_2) \mod 2$

   (b) $((1 + x_1) \cdot (1 + x_2) + (1 + x_1) \cdot x_2 + x_1 \cdot (1 + x_2) + x_1 \cdot x_2) \mod 2$

   (c) $((1 + x_1) \cdot (1 + x_2) \cdot (1 + x_3) + (1 + x_1) \cdot x_2 \cdot x_3 + x_1(1 + x_2) \cdot (1 + x_3) + x_1 \cdot x_2 \cdot x_3) \mod 2$

   (d) $((1 + x_1) \cdot (1 + x_2) \cdot x_3 + (1 + x_1) \cdot x_2 \cdot (1 + x_3) + (1 + x_1) \cdot x_2 \cdot x_3 + x_1 \cdot (1 + x_2) \cdot x_3 + x_1 \cdot x_2 \cdot (1 + x_3)) \mod 2$

2. (a) 11101

   (b) 000000

   (c) 000000

3. If $y_1y_2y_3y_4 = x_3x_2x_4x_1$ then $x_1x_2x_3x_4 = y_4y_2y_1y_3$. So $f^{-1}(y_1y_2y_3y_4) = y_4y_2y_1y_3$.

4. D is the inverse of E in the x variable. To find it, let $y_1y_2 = x_2x_1 \oplus k_1k_2$. Then $x_1 + k_2 \equiv y_2 \mod 2$ and $x_2 + k_1 \equiv y_1 \mod 2$. So $x_1 \equiv y_2 + k_2 \mod 2$ and $x_2 \equiv y_1 + k_1 \mod 2$. This means $x_1x_2 = y_2y_1 \oplus k_2k_1$. So $D(y_1y_2, k_1k_2) = y_2y_1 \oplus k_2k_1$ satisfies the desired identity: with $y_1y_2 = E(x_1x_2, k_1k_2) = x_2x_1 \oplus k_1k_2$, we get

$$\begin{aligned} D(E(x, k), k) &= y_2y_1 \oplus k_2k_1 \\ &= (x_1x_2 \oplus k_2k_1) \oplus k_2k_1 \\ &= x_1x_2 = x. \end{aligned}$$

[1] Slogan on posters during Word War II.

5. (a) 4, (b) -5, (c) 11 (d) 2, (e) 0, (f) 2.30259, (g) 0.693147 (h) 5.35755, (i) 2.00432, (j) 22, (k) -7, (l) 2/3, (m) 5, (n) 46/15, (o) 16/15

6. (a) Domain all real numbers; range all positive real numbers. 64, 128, 256, $\frac{1}{2}$, $\frac{1}{16}$, 11.4716, 0.033262.

   (b) Domain all integer; range $= \{1, 2, 3, 4, 5, 6\}$. 1, 3, 2, 6, 4, 5, 1.

   (c) Domain all positive reals; range all reals. 0, 1, 2, 3, -2, -5, 0.49714.

   (d) Domain all strings; range = nonnegative integers.

$$\begin{aligned} k(\texttt{Y2K}, \texttt{Y2K}) &= 0, \\ k(\texttt{SUMMER}, \texttt{SUMMER}) &= 1, \\ k(\texttt{IDEOLOGICAL}, \texttt{IDEOLOGIQUE}) &= 3 \\ k(\texttt{11011101}, \texttt{00100010}) &= 8 \end{aligned}$$

   (e) Domain all persons with telephone numbers; range all strings of digits assigned to telephone customers. E.g., if X. Y. Zee's phone number is $123-456-7890$, then $T(\text{X. Y. Zee}) = 123-456-7890$.

   (f) Domain all reals; range all reals. 0, 0.35, -0.4, 4743.32.

7. (a) 2, 5, 23, $-\frac{13}{16}$

   (b) -1, -3, 0, 17, 0, -399

8. (a) $\ln\left(5^{10000}\right) = 10000 \ln 5 = 160944$

   (b) $\log_2\left(3^{-84371}\right) = -84371 \cdot (1.58496) = -133725$

   (c) $x \ln 2 < 7 \ln 10$, so $x < (7 \ln 10)/(\ln 2) = 23.2535$. Largest integer x is 23.

   (d) $13 \ln 3 \le x \ln 4$; $x \ge (13 \ln 3)/(\ln 4) = 10.3023$. Smallest integer x is 11.

9.

$$\begin{aligned} \left\lfloor \log_{10}\left(3^{3141592}\right) \right\rfloor + 1 &= \lfloor 3141592 \ln 3 / \ln 10 \rfloor + 1 \\ &= \lfloor 1498920.3169 \rfloor + 1 \\ &= 1498921 \end{aligned}$$

10. (a) $f(x) = (-1)^n$

(b) $g(n) = \lfloor \log_{10}(\sqrt{n}) \rfloor + 1$

(c) $w(n) = 26^n$

(d) $v(n) = n^4$

11.

n	$\pi(n)$	n	$\pi(n)$	n	$\pi(n)$	n	$\pi(n)$	n	$\pi(n)$	n	$\pi(n)$	n	$\pi(n)$
2	1	9	4	16	6	23	9	30	10	37	12	44	14
3	2	10	4	17	7	24	9	31	11	38	12	45	14
4	2	11	5	18	7	25	9	32	11	39	12	46	14
5	3	12	5	19	8	26	9	33	11	40	12	47	15
6	3	13	6	20	8	27	9	34	11	41	13	48	15
7	4	14	6	21	8	28	9	35	11	42	13	49	15
8	4	15	6	22	8	29	10	36	11	43	14	50	15

12.

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
2	1	9	6	16	8	23	22	30	8	37	36	44	20
3	2	10	4	17	16	24	8	31	30	38	18	45	24
4	2	11	10	18	6	25	20	32	16	39	24	46	22
5	4	12	4	19	18	26	12	33	20	40	16	47	46
6	2	13	12	20	8	27	18	34	16	41	40	48	16
7	6	14	6	21	12	28	12	35	24	42	12	49	42
8	4	15	8	22	10	29	28	36	12	43	42	50	20

13. Since p and q are distinct we can list all the numbers in the range 1 to pq that have a factor in common with p and q: p, $2p$, $3p$, ..., qp, and q, $2q$, $3q$, ..., $(p-1)q$, pq. These lists contain, respectively, q, and p numbers, but pq appears in each list. Thus there are $p+q-1$ numbers in the range 1 to pq that have a factor in common with one or the other. Then the total number of values relatively prime to pq is $pq-(p+q-1) = pq-p-(q-1) = p(q-1)-(q-1) = (q-1)(p-1)$.

3.3

1. (a) At worst, n comparisons; at best, 1.

   (b) At best n comparisons will be needed.

2. The logarithm base conversion formula explains this.

3. Pick a positive a and a positive C. Then, for all sufficiently large values of n, $\ln(C) + n\ln(a) \leq n\ln(n)$. That is, $\ln(C \cdot a^n) \leq \ln(n^n)$, or $C \cdot a^n \leq n^n$ for all sufficiently large n. This means that $n^n \notin \mathcal{O}(a^n)$ for any a.

5. $\mathcal{O}\left(10^{100}\right) \subset \mathcal{O}(\ln(n)) = \mathcal{O}(\log_{10}(n)) \subset \mathcal{O}(n^3) = \mathcal{O}\left(n^3 + n^2\right) \subset \mathcal{O}\left(n^{100}\right) \subset \mathcal{O}\left(1.1^n\right) \subset \mathcal{O}\left(3^n\right) \subset \mathcal{O}\left(n2^n\right) \subset \mathcal{O}(n!)$.

6. If $\mu(n) \in \mathcal{O}\left(a^n\right)$, then there is are constants M and N such that $|\mu(n)| \leq Ma^n < Mb^n$ for all $n \geq M$. $\mu(n) = b^n$ is not in $\mathcal{O}\left(a^n\right)$: if it were, then there would be M and N such that $b^n \leq Ma^n$ for all $n \geq N$. This would mean that $(b/a)^n \leq M$ for all $n \geq N$, which is impossible since $b/a > 1$ and the sequence $(b/a)^n$ goes to ∞.

3.4

1. `0000111 0010010 0011111 0011000`

2. `SELL STOCK`

3. (a) 10101110110001111100110100100000
   (b) 0001011
   (c) 00000100101100111111000110111010 1
   (d) 00011111000110111010100001001011

4. (a) $b_4 = b_3 + b_1$, (b) $b_4 = b_3 + b_2 + b_1$

6. (a) $b_5 = b_4 + b_1$, period 15, (b) $b_5 = b_3 + b_1$, period 31

7. No for 3, 4, 5; zero initial state implies zero forever.

8. $C(9, 2) = 36$

9.
```
1 0 1 1
0 1 1 0
1 1 0 1
1 0 1 0
0 1 0 0
1 0 0 1
0 0 1 0
0 1 0 1
1 0 1 1
```
   period 8

3.5

1. `AH` in binary ASCII and subdivided into 4-bit blocks is 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0. Enciphering with $k = 001$ gives 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0.

2. In reprints after March 2002, the following is exercise 2.

(a) Let $f_{k_1k_2k_3}(x_1x_2)$ be the function defined on page 224, and let $F_k(x)$ be the corresponding Feistel function, whose formula is given at the bottom of page 224. Calculate $F_{101}(1001)$ and verify that the formula for $F_k^{-1}(x)$, given by $F_k^{-1}(y_1y_2y_3y_4) = ((y_3y_4) \oplus f_k(y_1y_2))||y_1y_2$, applied to this value recovers 1001.

(b) Let $f_k(x)$ be the 3-bit-valued function defined by $f_{k_1k_2}(x_1x_2x_3) = (k_2 \cdot x_1 \text{ MOD } 2)((k_1 \cdot x_2 + 1) \text{ MOD } 2)((k_1 \cdot k_2 \cdot x_1 + x_3) \text{ MOD } 2)$, and let $F_k(x)$ be the corresponding 6-bit-valued Feistel function, $F_k(x)$, where $k = k_1k_2$ is a 2-bit key and $x = x_1x_2x_3x_4x_5x_6$ is a 6-bit plaintext. Compute $F_{11}(001100)$. Use the formula at the bottom of page 225 to compute F_{11}^{-1} on the value obtained and verify that it recovers the original string 001100.

A solution to this exercise is as follows.

(a) $F_{101}(1001) = (01)||(10 \oplus f_{101}(01))$

Now

$$\begin{aligned} f_{101}(01) &= \left(1 + 1 \cdot 0^2 + 0 \cdot 0 \cdot 1 \text{ MOD } 2\right)\left(1^2 \cdot 0 \cdot 1 + 1 \cdot 1^2 \text{ MOD } 2\right) \\ &= 11 \end{aligned}$$

so

$$\begin{aligned} F_{101}(1001) &= (01)||(10 \oplus 11) \\ &= (01)||(01) \\ &= 0101 \end{aligned}$$

Also

$$F_{101}^{-1}(0101) = (01 \oplus f_{101}(01))||(01).$$

Since

$$f_{101}(01) = \left(1 + 1 \cdot 0^2 + 0 \cdot 0 \cdot 1 \text{ MOD } 2\right)\left(1^2 \cdot 0 \cdot 1 + 1 \cdot 1^2 \text{ MOD } 2\right)$$

$$= \quad 11,$$

$$\begin{aligned} F_{101}^{-1}(0101) &= (01 \oplus 11)||01 \\ &= (10)||(01) \\ &= 1001. \end{aligned}$$

(b) $R(x) = 100$, $L(x) = 001$, and

$$\begin{aligned} f_{11}(R(x)) &= f_{11}(100) \\ &= (1 \cdot 1)(1 \cdot 0 + 1)(1 \cdot 1 \cdot 1 + 0) \\ &= 111 \end{aligned}$$

Then

$$\begin{aligned} F_{11}(001100) &= (100)||(001 \oplus 111) \\ &= (100)||(110) \\ &= 100110. \end{aligned}$$

3. (a) $y_0 = F_k(iv \oplus x_0)$, $y_i = F_k(y_{i-1} \oplus x_i)$, $i = 1, 2, \ldots$.
   (b) $x_0 = iv \oplus F_k^{-1}(y_0)$, $x_i = y_{i-1} \oplus F_k^{-1}(y_i)$, $i = 1, 2, \ldots$.

4. $Y_1 = F_k(iv)$, $x_1 = y_1 \oplus L_m(Y_1)$; $Y_i = F_k(S(y_{i-1}, y_{i-1}))$, $x_i = y_i \oplus L_m(Y_i)$, $i = 1, 2, \ldots$.

5. $F_{k_1k_2}^{-1}(y_1y_2y_3y_4) = \left(y_3 + k_1k_2y_1 + k_1y_2^2\right)(y_4 + k_1y_1y_2 + k_2y_1y_2)(y_1)(y_2) \mod 2$.

3.6

1. `VWNLB`

2. (a) is likely uncorrupted; (b) is corrupted; (c) is likely uncorrupted; (d) is corrupted.

3. `HELLO WORLD`

   (a) 26^5; $26^5/26^{10} = 1/26^5$.
   (b) 26^{10}; $26^{10}/26^{15} = 1/26^5$.
   (c) 26^{5n-5}; $26^{5n-5}/26^{5n} = 1/26^5$.

4. The messages 00000000 00000000 10110101 and 00000000 01111010 10110101 hash to the same value.

4.1

1. See the table of primes.

2. The numbers 1328 through 1360 are all composite.

3. $n!$ is divisible by 2, 3, ..., n, so $n! + 2$, $n! + 3$, $n! + 4$, ..., $n! + (n - 1)$, $n! + n$ are all divisible by 2, ..., n.

4. (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151), (179, 181), (191, 193), (197, 199), (227, 229), (239, 241), (269, 271), (281, 283), (311, 313), (347, 349), (419, 421), (431, 433), (461, 463), (521, 523), (569, 571), (599, 601), (617, 619), (641, 643), (659, 661), (809, 811), (821, 823), (827, 829), (857, 859), (881, 883), (1019, 1021), (1031, 1033), (1049, 1051), (1061, 1063), (1091, 1093), (1151, 1153), (1229, 1231), (1277, 1279), (1289, 1291), (1301, 1303), (1319, 1321), (1427, 1429), (1451, 1453), (1481, 1483), (1487, 1489), (1607, 1609), (1619, 1621), (1667, 1669), (1697, 1699), (1721, 1723), (1787, 1789), (1871, 1873), (1877, 1879), (1931, 1933), (1949, 1951), (1997, 1999), (2027, 2029), (2081, 2083), (2087, 2089), (2111, 2113), (2129, 2131), (2141, 2143), (2237, 2239), (2267, 2269), (2309, 2311), (2339, 2341), (2381, 2383), (2549, 2551), (2591, 2593), (2657, 2659), (2687, 2689), (2711, 2713), (2729, 2731), (2789, 2791), (2801, 2803), (2969, 2971), (2999, 3001), (3119, 3121), (3167, 3169), (3251, 3253), (3257, 3259), (3299, 3301), (3329, 3331), (3359, 3361), (3371, 3373), (3389, 3391), (3461, 3463), (3467, 3469), (3527, 3529), (3539, 3541), (3557, 3559), (3581, 3583), (3671, 3673), (3767, 3769), (3821, 3823), (3851, 3853), (3917, 3919), (3929, 3931), (4001, 4003), (4019, 4021), (4049, 4051), (4091, 4093), (4127, 4129), (4157, 4159), (4217, 4219), (4229, 4231), (4241, 4243), (4259, 4261), (4271, 4273), (4337, 4339), (4421, 4423), (4481, 4483), (4517, 4519), (4547, 4549), (4637, 4639), (4649, 4651), (4721, 4723), (4787, 4789), (4799, 4801), (4931, 4933), (4967, 4969), (5009, 5011), (5021, 5023), (5099, 5101), (5231, 5233), (5279, 5281), (5417, 5419), (5441, 5443), (5477, 5479), (5501, 5503), (5519, 5521), (5639, 5641), (5651, 5653), (5657, 5659), (5741, 5743), (5849, 5851), (5867, 5869), (5879, 5881), (6089, 6091), (6131, 6133), (6197, 6199), (6269, 6271), (6299, 6301), (6359, 6361), (6449, 6451), (6551, 6553), (6569, 6571), (6659, 6661), (6689, 6691), (6701, 6703), (6761, 6763), (6779, 6781), (6791, 6793), (6827, 6829), (6869, 6871), (6947, 6949), (6959, 6961), (7127,

7129), (7211, 7213), (7307, 7309), (7331, 7333), (7349, 7351), (7457, 7459), (7487, 7489), (7547, 7549), (7559, 7561), (7589, 7591), (7757, 7759), (7877, 7879), (7949, 7951), (8009, 8011), (8087, 8089), (8219, 8221), (8231, 8233), (8291, 8293), (8387, 8389), (8429, 8431), (8537, 8539), (8597, 8599), (8627, 8629), (8819, 8821), (8837, 8839), (8861, 8863), (8969, 8971), (8999, 9001), (9011, 9013), (9041, 9043), (9239, 9241), (9281, 9283), (9341, 9343), (9419, 9421), (9431, 9433), (9437, 9439), (9461, 9463), (9629, 9631), (9677, 9679), (9719, 9721), (9767, 9769), (9857, 9859), (9929, 9931), (10007, 10009), (10037, 10039), (10067, 10069), (10091, 10093), (10139, 10141), (10271, 10273), (10301, 10303), (10331, 10333), (10427, 10429), (10457, 10459), (10499, 10501), (10529, 10531), (10709, 10711)

6. (a) $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$, (b) $6517 = 7^3 \cdot 19$, (c) $961 = 31^2$ (d) $371293 = 13^5$

7.

n	$n!$	factorization
2	2	2
3	6	$2 \cdot 3$
4	24	$2^3 \cdot 3$
5	120	$2^3 \cdot 3 \cdot 5$
6	720	$2^4 \cdot 3^2 \cdot 5$
7	5040	$2^4 \cdot 3^2 \cdot 5 \cdot 7$
8	40320	$2^7 \cdot 3^2 \cdot 5 \cdot 7$
9	362880	$2^7 \cdot 3^4 \cdot 5 \cdot 7$
10	3628800	$2^8 \cdot 3^4 \cdot 5^2 \cdot 7$
11	39916800	$2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$
12	479001600	$2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$
13	6227020800	$2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$

8. (a) 25; no; $73 \cdot 137$; (b) 1229

10. $23981204798221 = 15485863 \cdot 15485867$

11. (a) 15; (b) 23; (c) 61; (d) 1

12. (a) $17^{-1} \equiv 53 \pmod{60}$
    (b) $25^{-1} \equiv 57 \pmod{89}$
    (c) $3^{-1} \equiv 44 \pmod{131}$
    (d) $131^{-1} \equiv 2 \pmod{3}$

(e) $1006^{-1} \equiv 3918816 \pmod{7233631}$

13. (a) $x = 17$; (b) $x = 19$; (c) $x = 48$

14. (a) $x = 12y \mod 13$; (b) $x = (41+39)y \mod 81$; (c) $x = 9y \mod 17$

15. (a) $(2-1)! \equiv 1 \equiv -1 \pmod{2}$, $(3-1) \equiv 2 \equiv -1 \pmod{3}$, and so on.

    (b) $(n-1)! = [2 \cdot 3 \cdot 4 \cdot \cdots \cdot (n-3) \cdot (n-2)] \cdot (n-1)$, and by the exercise mentioned in the Hint, each of the factors in the brackets has an inverse modulo n distinct from itself. So, somewhere in the product is the inverse of 2, somewhere else is the inverse of 3, and so on. Each number in the range 2 to $(n-2)$ is multiplied by its multiplicative inverse, so when this product is reduced modulo n, the quantity in brackets reduces to 1. Thus $(n-1)! \equiv 1 \cdot (n-1) \equiv -1 \pmod{n}$.

    (c) (i) If $n = 4$, then $(n-1)! = 6$, which is not congruent to -1 modulo 4. (ii) If n factors into distinct factors, then $n = r \cdot s$, where $r \neq s$. Since both r and s are less than $n-1$, they both appear as factors in $(n-1)!$, so n divides $(n-1)!$. (iii) If n is a square of a prime p at least 3, then $(n-1)! = 1 \cdot 2 \cdot \cdots \cdot p \cdot (p+1) \cdot \cdots \cdot (2p-1) \cdot 2p \cdot (2p+1) \cdot \cdots \cdot (n-1)$. Since the factors p and $2p$ appear in $(n-1)!$, this number is divisible by p^2, which is n.

    (d) In the worst case $179424673 - 2 = 179424671$ multiplications and divisions would be needed. In general, if we measure the size of the input to this algorithm by the number of decimal digits n in the representation of the number, then the worst case computational expense function for this primality testing algorithm is $\mathcal{O}(10^n)$, where we count a step as being a multiplication and reduction modulo n.

16. 2, 3, 5, 11, 23, 29, 41, 53, 83, 89

17. (a) 3, 7, 31, 127

    (b) and (c) If $n = r \cdot s$, where r and s are greater than 1, then $2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1) \cdot ((2^r)^{s-1} + (2^r)^{s-2} + \cdots + 1)$, which is a factorization of $2^n - 1$ into nontrivial factors.

4.2

1. (a) 12, 13, 27, 55, 111, 219, 450 is superincreasing.

(b) 4, 15, 18, 36, 72, 145 is not.

(c) 17, 18, 39, 69, 180, 331 is not.

(d) 1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683 is superincreasing.

2. (a) 2725; (b) 377; (c) 7179

3. (a) 310 cannot be written as a sum of a subset of the sequence.

(b) 1, 1, 1, 1, 1, 1, 1, 0

(c) 127 cannot be written as a sum of a subset of the sequence.

(d) 1, 1, 1, 0, 0, 0, 0, 1

(e) 1, 1, 1, 1, 1, 1, 1, 1

4. 3913, 4004, 173, 2166, 5679, 4997, 5717, 5146

5. 20, 40, 75, 145, 305, 625, 226, 482

6. 336

7. 1, 1, 1, 0, 0, 1, 0, 1

8. 0, 1, 1, 0, 1, 0, 0, 0

9. 00110110

10. $n-1$

11. 9584, 11616, 9584, 1824, 1824, 7760, 9584, 9424, 1824, 11616, 1824, 15104, 1824, 15104, 1824, 3488

12. The pattern of sum representations is 1, 2, 3, ..., n, $n+1$, $n+2$, ..., $n+(n-1)=2n-1$, $n+(n-1)+1=2n$, $n+(n-1)+2=2n+1$, ..., $n+(n-1)+(n-2)=3n-3$, $n+(n-1)+(n-2)+1=3n-2$, ... The largest possible number representable by a subset sum is $1+2+3+\cdots+n=n(n+1)/2$.

13. Use the identity that $r^n-1=(r-1)(r^{n-1}+r^{n-2}+\cdots+r^3+r^2+r+1)$.

4.3

1. (a) 3; (b) 13; (c) 25; (d) 5; (e) 46

2. (a) 99; (b) 1; (c) 1; (d) 1; (e) 1; (f) 100

3. $56 = 3 \cdot 16 + 8$, so by Fermat's Little Theorem, since 17 is prime,

$$\begin{aligned} 2^{56} + 3^{56} &\equiv 2^{3\cdot 16+8} + 3^{3\cdot 16+8} \\ &\equiv (2^3)^{16} \cdot 2^8 + (3^3)^{16} \cdot 3^8 \\ &\equiv 1 \cdot 2^8 + 1 \cdot 3^8 \\ &\equiv 2^8 + 3^8 \pmod{17}. \end{aligned}$$

   Now $2^2 \equiv 4 \pmod{17}$, $2^4 \equiv 4^2 \equiv 16 \equiv -1 \pmod{17}$, and $2^8 \equiv (-1)^2 \equiv 1 \pmod{17}$; $3^2 \equiv 9 \pmod{17}$, $3^4 \equiv 9^2 \equiv 81 \equiv 13 \pmod{17}$ and $3^8 \equiv 13^2 \equiv 169 \equiv 16 \pmod{17}$. So

$$\begin{aligned} 2^{56} + 3^{56} &\equiv 2^8 + 3^8 \\ &\equiv 1 + 16 \\ &\equiv 17 \equiv 0 \pmod{17} \end{aligned}$$

4. (a) $a \equiv b \pmod{m}$ means that $a - b = rm$ for some integer m. Multiplying by k gives $ka - kb = km$, which means that $ka \equiv kb \pmod{km}$.

   (b) Because 23 is prime, by Fermat's Theorem, $14^{23} \equiv 14 \pmod{23}$. By part (a), $5 \cdot 14^{23} \equiv 5 \cdot 14 \pmod{5 \cdot 23}$. That is, $5 \cdot 14^{23} \equiv 70 \pmod{115}$.

5. Let $r_1, r_2, \ldots, r_{\phi(n)}$ be the numbers in the range $1, \ldots, n-1$ that are relatively prime to n. For a relatively prime to n, all of the numbers $a \cdot r_1 \bmod n$, $a \cdot r_2 \bmod n$, $\ldots$, $a \cdot r_{\phi(n)} \bmod n$ are distinct from one another, so they are just a reordering of $r_1, \ldots, r_{\phi(n)}$. Thus $(a \cdot r_1 \bmod n) \cdot (a \cdot r_2 \bmod n) \cdots (a \cdot r_{\phi(n)} \bmod n) \equiv r_1 \cdots r_{\phi(n)} \pmod{n}$. This becomes $a^{\phi(n)} \cdot (r_1 \cdot r_2 \cdots r_{\phi(n)}) \equiv (r_1 \cdot r_2 \cdots r_{\phi(n)}) \pmod{n}$. Cancel the quantity in parenthesis from both sides to yield the desired identity.

6. By Exercise 5, $a^{\phi(n)} \bmod n = a$. If $e = q\phi(n) + r$, where $0 \leq r < \phi(n)$, then $a^e \bmod n = a^{q\phi(n)+r} \bmod n = (a^q)^{\phi(n)} \cdot a^r \bmod n = 1 \cdot a^r \bmod n$. This is equivalent to saying that $a^e \equiv a^r \pmod{n}$, or $a^e \bmod n = a^{e \bmod \phi(n)} \bmod n$.

7. (a) First note that $\phi(15) = (5-1)(3-1) = 8$. Then (a) $D(E(x)) = (x^3)^3 \text{ MOD } 15 = x^9 \text{ MOD } 15 = x^{9 \text{ MOD } 8} \text{ MOD } 15 = x^1 \text{ MOD } 15 = x$ for all x relatively prime to 15, by the previous exercise.

8. (5, 5), (7, 7), (11, 11), (13, 13), (17, 17), (19, 19), (23, 23)

9. a is relatively prime to pq, so it has an inverse a^{-1} modulo pq. By definition, a^{-t} means $(a^{-1})^t$. In the proof of part (2), if a is not relatively prime to pq, then it has no inverse modulo pq.

10. (a) Multiply $a^{p-1} \equiv 1 \pmod{p}$ by a^{-1}.

    (b) The largest r such that $2^r \leq p-2$ is $R = \lfloor \log_2(p-2) \rfloor$. Computing $a^{2^1} \text{ MOD } p$, $a^{2^2} \text{ MOD } p$, ..., $a^{2^R} \text{ MOD } p$ takes R multiplications (squarings). Then $p-2 = c_R 2^R + c_{R-1} \cdot 2^{R-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2^1 + c_0$ where c_i is 0 or 1. So $a^{p-2} = a^{c_R 2^R + c_{R-1} \cdot 2^{R-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2^1 + c_0} = a^{c_R \cdot 2^R} \cdot a^{c_{R-1} 2^{R-1}} \cdot \cdots \cdot a^{c_2 \cdot 2^2} \cdot a^{c_1 \cdot 2} \cdot a^{c_0}$, which requires a multiplication only for $c_i = 1$. Thus at most R multiplications are needed for the second phase. Thus, a total of $R + R = 2R$ multiplications are needed.

11. $561 = 3 \cdot 11 \cdot 17$ $1105 = 5 \cdot 13 \cdot 17$, $2821 = 7 \cdot 13 \cdot 31$, $10585 = 5 \cdot 29 \cdot 73$, $15841 = 7 \cdot 31 \cdot 73$, $29341 = 13 \cdot 37 \cdot 61$

4.4

1. (a) 329 236 (b) 386 968 (c) 035 450

2. (a) `TELL` (b) `QUIT` (c) `FIRE`

3. `TAKE TWO`

4. (a) 22 681 (b) 14 248 (c) 05 589

5. (a) 10 164=`PAY`; (b) 05 118=`HOW`

6. 6712 5879 2989

7. `DONT WORRY BE HAPPY`

8. $p = 1741$, $q = 6827$, `CLEAR`

9. (a) $n = pq - p - q + 1$, so $p + q = pq - n + 1$; that is, $p + q = m - n + 1$.

(b) Since $q = m/p$, substituting into the equation in (a) eliminates q: $p + (m/p) = m - n + 1$; multiplying through by p gives $p^2 + m = (m - n + 1)p$, so p satisfies $p^2 - (m - n + 1)p + m = 0$.

(c) By the quadratic formula,

$$p = \frac{(m - n + 1) + \sqrt{(m - n + 1)^2 - 4m}}{2}.$$

Substituting this into $q = m/p$ gives

$$q = \frac{(m - n + 1) - \sqrt{(m - n + 1)^2 - 4m}}{2}.$$

(d) $m = 2039 \cdot 2617$

10. (a) By the theorem, there exist s and t, which are found by the extended Euclidean algorithm, such that $1 = se_a + te_z$. Thus $x \equiv x^1 \equiv x^{se_a + te_z} \equiv (x^{e_a})^s \cdot (x^{e_a})^t \pmod{m}$.

(b) $1 = 43 \cdot 47 - 20 \cdot 101$, so $x = 2467^{43} \cdot 2664^{-20} \equiv 1000 \pmod{m}$.

4.5

1. (a)

x	2^x	3^x	4^x	5^x	6^x	7^x	8^x	9^x	10^x
1	2	3	4	5	6	7	8	9	10
2	4	9	5	3	3	5	9	4	1
3	8	5	9	4	7	2	6	3	10
4	5	4	3	9	9	3	4	5	1
5	10	1	1	1	10	10	10	1	10
6	9	3	4	5	5	4	3	9	1
7	7	9	5	3	8	6	2	4	10
8	3	5	9	4	4	9	5	3	1
9	6	4	3	9	2	8	7	5	10
10	1	1	1	1	1	1	1	1	

(c) 2, 6, 7, 8

2. (a) $x = 6$

(b) $x = 2, 3, 4, \ldots, 11$

(c) $x = 10$

(d) 3, 9, 15, 21

3. 6, 36, 31, and 1 are the only numbers that turn up as powers of 6, modulo 37. Since 36 is its own inverse, modulo 37, raising it to any even power will give 1. Raising 6 to an even exponent will then give either 36 or 1. It would be better to choose s relatively prime to 36– e.g., $s = 11$.

4. 128

5. Bob calculates $21^6 \mod 23$, which is 18. This is the shift amount used to encipher the text, so he will use an 8-shift to decipher: `STAYAWAKE`.

6. (a) $(t, y) = (49, 25)$
   (b) $(t, y) = 27, 63)$

7. (a) $x = 33$
   (b) $x = 2$

8. (a) $(t, y) = (908, 989)$
   (b) $(t, y) = (347, 777)$.

9. (b) $x = 529$
   (c) $x = 421$

10. (a) (11359, 6319), (7829, 10369), (514, 69)
    (b) `ILO VEY OUX`

11. By Fermat's Little Theorem, $t^{p-1-a} \equiv t^{p-1}t^{-a} \equiv 1 \cdot t^{-a} \equiv t^{-a} \pmod{p}$.

12. $s = p - 1$ would make s^a take either the value 1 or $p - 1$.

4.6

1. (a) $\sigma = 70$
   (b) He regards the pair as likely to be authentic since $54^7 \mod 91 = 89$.

2. (a) (185, 21)
   (b) $\tilde{x} = 44$, $\tilde{\sigma} = 86$ Is this a valid message-signature pair? yes, because $\tilde{\sigma}^{e_A} \mod 91 = 86^7 \mod 91 = 44$

3. The first is valid; the second is not.

4. 8338987

5. 525

6. Yes. $463^{23} \equiv 240 \pmod{1271}$, which is 11110000 in binary.

4.7

1., 2., and 3 are given in the following table.

n	n^2 MOD 39	n^2 MOD 32	n^2 MOD 31	n	n^2 MOD 39	n^2 MOD 32	n^2 MOD 31
0	0	0	0	20	10	16	28
1	1	1	1	21	12	25	7
2	4	4	4	22	16	4	19
3	9	9	9	23	22	17	2
4	16	16	16	24	30	0	18
5	25	25	25	25	1	17	5
6	36	4	5	26	13	4	25
7	10	17	18	27	27	25	16
8	25	0	2	28	4	16	9
9	3	17	19	29	22	9	4
10	22	4	7	30	3	4	1
11	4	25	28	31	25	1	
12	27	16	20	32	10		
13	13	9	14	33	36		
14	1	4	10	34	25		
15	30	1	8	35	16		
16	22	0	8	36	9		
17	16	1	10	37	4		
18	12	4	14	38	1		
19	10	9	20				

4. $(n-x)^2 \equiv n^2 - 2nx + x^2 \equiv 0 - 0 + x^2 \pmod{n}$.

5.

Round	r commit-ment	$w \equiv r^2$ wit-ness	e chal-lenge	$y \equiv r \cdot s^e$ re-sponse	$z \equiv y^2$ compa-rison 1	$z' \equiv w \cdot v^e$ compa-rison 2
1	26	676	1	2938	2604	2604
2	519	1557	0	519	1557	1557
3	1040	2945	1	5935	560	560
4	2804	6832	1	4414	655	655
5	5991	6345	1	34	1156	1156
6	6263	6761	0	6263	6761	6761
7	1118	172	1	7310	1763	1763
8	4309	7176	0	4309	7176	7176

5.1

1. The cryptographic application stored on a computer disk can be modified by an opponent from a remote site. The modified application could leak key information or do other damaging work. If the cryptographic application is implemented in circuitry, then the opponent must mount a more daring attack of finding the physical device and either replacing or modifying it.

2. The inverse of $f_k(x)$ given in (5.1) is obtained merely by "subtracting" $F(k, R(x))$ from the left half of the bit string, that is, XOr-ing the left half of $f_k(x)$ with $F(k, R(x))$. This is precisely what f_k itself does.

3. (a) Taking the base 10 logarithm of Stirling's formula and using properties of logarithms, we obtain $\log_{10}(n!) \approx ((n + .5)\ln(n) - n + \ln(2\pi)/2)/\ln(10)$. Substituting $n = 2^{64}$, we get $\log_{10}(2^{64}) \approx 3.474\times10^{20}$, which says that $2^{64}! \approx 10^{3.474\times10^{20}} = 2.951\times10^{10^{20}-3} \approx 2.951\times10^{10^{20}}$; there are on the order of $10^{20} = 100000000000000000000$ *digits* in the decimal representation of this number!

   (b) It is about $2^{56}/2.951\times10^{10^20} = 7.2\times10^{16}/2.951\times10^{10^20} = 2.779\times 10^{16-10^{20}} \approx 2.779 \times 10^{-10^{20}}$, an unimaginably small number.

   (c) Highly unlikely.

4. $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

5. $\mathrm{IP}^{-1}(x_1x_2x_3x_4x_5x_6x_7x_8) = x_4x_1x_3x_5x_7x_2x_8x_6$

7. (b) 1011101110 is the key.