1.— Certificates are primarily a solution for
a) distributing symmetric keys
b) distributing computation
c) distributing trust

2.— Confidentiality could be compared to
a) putting letters inside an envelope
b) using invisible ink
c) signing documents

3.— PayWord is based on
a) hash functions
b) symmetric cryptography
c) public-key cryptography

4.— The best known algorithms for factoring large integers have, with respect to the logarithm of an integer to factor,
a) polynomial time complexities
b) superpolynomial time complexities
c) non-elementary time complexities

5.— CA stands for
a) Certification Authority
b) Cryptographic Algorithm
c) Central Arbitrer

6.— The key length of a Vigenére cipher can be found out easily by applying
a) differential cryptanalysis
b) statistics of the underlying language
c) autocorrelation measurements

7.— The number of elements in Z_p^*, when p is a prime number, is
a) $p+1$
b) $p-1$
c) p

8.— ECB stands for
a) Encrypted Chained Block
b) Encrypted Cipher Block
c) Electronic Code Book

9.— Message integrity denotes preserving
a) transmission cost
b) secrecy
c) content

10.— If S is a finite set and μ a random mapping $\mu : S \to S$, then the average length of a cycle $s, \mu(s), \mu^2(s), \ldots, s$ is around
a) $|S|$
b) $\sqrt[3]{|S|}$
c) $\sqrt{|S|}$

11.— $a \cdot a^{-1} \pmod p$ equals
a) $1 \pmod p$
b) $a \pmod p$
c) $0 \pmod p$

12.— The Euclid's Algorithm is based on the recurrence
a) $\gcd(a,b) = \gcd(a \bmod b, a)$
b) $\gcd(a,b) = \gcd(b, a \bmod b)$
c) $\gcd(a,b) = \gcd(b, a-b)$

13.— A way to perform zero knowledge proofs non-interactively can be obtained from
a) a secret sharing scheme
b) oblivious transfer
c) cryptographic coin flips

14.— A language that has high redundancy
a) cannot be encrypted securily
b) can be compressed significantly
c) is difficult to predict

15.— SHA stands for
a) Secure Hash Algorithm
b) Standard Hash Algorithm
c) Secret Hash Algorithm

16.— Shamir's secret sharing method is based on
a) CRT
b) polynomial interpolation
c) oblivious transfer

17.— A playback attack can be targeted against
a) a block cipher
b) a self-synchronous stream cipher
c) a synchronous stream cipher

18.— The key stream from a strong stream cipher
a) does not compress well
b) has nontrivial autocorrelation
c) has more ones and zeros

19.— Let G be a set, $\circ$ a binary operation on G and $a, b, \ldots$ arbitrarily chosen elements of G. A necessary condition for $(G, \circ)$ to be a group is that
a) $\exists e : \forall a : e \circ a = a \circ e = e$
b) $a \circ b = b \circ a$
c) $(a \circ b) \circ c = a \circ (b \circ c)$

20.— DES is
a) a hash function
b) a stream cipher
c) a block cipher

21.— If RSA is used as a signature scheme, the secret decryption exponent d is contained
a) in the signature generation key
b) nowhere
c) in the signature verification key

22.— The fast exponentiaton algorithm spends on calculating x^y
a) $O(\log_2 y)$ single multiplications
b) $O(\log_2 x + \log_2 y)$ single multiplications
c) $O(\log_2 x)$ single multiplications

23.— DSA is a based on the intractability of the
a) integer factoring problem
b) Diffie-Hellman problem
c) discrete logarithm problem

24.— SHA is based on
a) Tiger
b) RC4
c) MD5

25.— Choose the most powerful of the following cryptanalytic attacks:
a) chosen-plaintext attack
b) known-plaintext attack
c) ciphertext-only attack

26.— Steganography is the art of
a) detecting unlawful communications
b) hiding messages
c) preserving confidentiality

27.— RC4 is a
a) block cipher
b) hash function
c) stream cipher

28.— The Fiat-Shamir Protocol is a protocol for
a) authentication, based on X.509
b) key distribution, based on DH
c) identification, based on ZKPs

29.— The subliminal channel of DSA is based on
a) the random parameter k
b) the disrepancy in the sizes of p and q
c) the SHA hash function

30.— The f-function in a Feistel network
a) cannot be surjective
b) must be bijective
c) should be nonlinear

31.— The Diffie-Hellman key exchange is a solution to the
a) key setup problem
b) Byzantine agreement problem
c) discrete logarithm problem

32.— The birthday attack against a hash function whose output is n bits long has the average time complexity of
a) 2^{n-1}
b) 2^n
c) $2^{\frac{n}{2}}$

33.— A nonlinear Boolean function $f : \mathbb{B}^n \rightarrow \mathbb{B}$ (B denotes the domain of Boolean values) is such that $f(x_1, \ldots, x_n)$
a) cannot be written without using the Boolean AND-operator
b) cannot be written as a product of some of the arguments $x_1, \ldots, x_n$
c) cannot be written as $a_1 x_1 \oplus \cdots \oplus a_n x_n$ for some constant $a_1, \ldots, a_n$

34.— $\varphi(30)$ equals
a) 8
b) 29
c) 6

35.— The computational cost of doing brute-force search for a key that has n bits is
a) 2^n
b) $2^{\frac{n}{2}}$
c) n

36.— Modular arithmetics do not necessarily preserve the
a) assosiativity rule
b) cancellation rule
c) commutativity rule

37.— The XOR function $\oplus$ is
a) non-commutative
b) non-linear
c) linear

38.— The number of tappings in an LFSR with the connection polynomial $x^5 + x^2 + x^1 + 1$ is
a) 4
b) 3
c) 2

39.— Weak collision resistance means that it is difficult to find
a) weak collisions
b) strong collisions
c) pseudo-collisions

40.— A public RSA key consists of
a) a modulus plus two exponents
b) a modulus plus an exponent
c) two factors of a composite modulus

41.— The Discrete Logarithm Problem is to
a) calculate g from $g^x \equiv y \pmod{n}$
b) calculate x from $g^x \equiv y \pmod{n}$
c) calculate g^{xy} from $g^x, g^y \pmod{n}$

42.— The elements of $\mathbb{Z}_n^*$ form a group when the group operation is
a) multiplicatio modulo n
b) addition modulo n
c) exponentiation modulo n

43.— In DES, nonlinearity is implemented
a) in the S-boxes
b) in the key schedule
c) by the Feistel structure

44.— The modular inverse of 2 modulo 5 is
a) 4
b) 3
c) 2

45.— The zero-knowledge property is that
a) any party can create faked proof runs indistinguishable from real ones
b) a proof run cannot be observed by third parties
c) the probability of succeeding in faking a proof is zero

46.— Let G be a finite group and $x \in G$. Then $x^{|G|}$ equals to
a) anything
b) x
c) 1_G

47.— If p is a prime number then $\varphi(p)$ equals
a) $p-1$
b) p
c) $\varphi(p-1)$

48.— The avalanche speed of DES is around
a) $2^{51.3}$ keys
b) four rounds
c) 64 bits

49.— The salt in the conventional UNIX password system protects against
a) parallel brute-force attacks
b) brute-force attacks against single passwords
c) differential attacks

50.— DES stands for
a) Digest Encoding Standard
b) Double-Encrypting Stream
c) Data Encryption Standard

51.— Choose that of the following cryptanalytic attacks that is most difficult to carry out in practice:
a) a ciphertext-only attack
b) brute-force search
c) differential cryptanalysis

52.— Choose the strongest property of a hash function of the following:
a) weak collision resistance
b) strong collision resistance
c) one-wayness

53.— Zero-knowledge proofs are typically implemented by
a) interactive protocols
b) challenge-response protocols
c) public-key systems

54.— CRT stands for
a) Collaborative Random Toss
b) Cryptographic Research Task
c) Chinese Remainder Theorem

55.— Assume a public RSA key has modulus n and a message x is being encrypted with $x|n$. Then
a) decryption fails always
b) decryption fails with probability $\frac{1}{2}$
c) decryption works always

56.— The differential attack against DES
a) recovers the round key of the last round
b) recovers the round key of the second round
c) recovers the round key of the first round

57.— Cut-and-choose is related for instance to
a) blind signatures
b) prime number generation
c) cryptanalysis

58.— PFS stands for
a) Perturbative Factoring Sieve
b) Perfect Forward Secrecy
c) Publicly Faked System

59.— An undeniable signature is a signature that definition
a) just a digital signature as digital signatures cannot be denied by
b) can be verified only interactively
c) a signature that cannot be cracked in the next 1,000 years

60.— The small subgroup attack against Diffie-Hellman can be inhibited for example so that
a) the modulus n is chosen so that $n-1$ is prime
b) $|\langle g\rangle|$ is prime
c) g is chosen to be a prime number

61.— CBC stands for
a) Cipher Block Coalescing
b) Cipher Block Chaining
c) Cipher Block Corresponding

62.— The birthday paradox is related to
a) choosing two elements from a set
b) draws from a set, without replacement
c) draws from a set, with replacement

63.— IDEA stands for
a) International Data Encryption Algorithm
b) Ingenious Digital Encryption Asymmetry
c) Involutive Data Encipherment Apparatus

64.— If $H(X)$ denotes the entropy of X, a random variable, and $\langle X, Y\rangle$ is the joint random variable of X and Y, then a sufficient condition for $H(\langle X, Y\rangle) = H(X) + H(Y)$ to hold is that
a) X and Y are independent
b) X and Y have disjoint domains
c) X and Y have the same individual entropies

65.— The Shannon entropy corresponding to a toss of coin is
a) 0
b) 1
c) $\frac{1}{2}$

66.— A commutative encryption scheme E is such that
a) $E_x(y) = E_y(x)$
b) $E_a(x)|E_a(y) = E_a(x|y)$, where $|$ denotes concatenation
c) $E_a(E_b(x)) = E_b(E_a(x))$

67.— The generator g in the Diffie-Hellman key exchange must be chosen so that (n is the DH modulus)
a) g and n have common factors
b) g is small when compared to n
c) $|\langle g\rangle|$ is large

68.— RC4 produces key stream quantized as
a) 64-bit words
b) 8-bit bytes
c) single bits

69.— The Chinese Remainder Theorem is related to
a) linear equation systems in modular arithmetics
b) the Diffie-Hellman key exchange
c) calculating remainders of rational numbers

70.— The information-theoretically secure symmetric cipher is called
a) one time pad
b) Vigenére cipher
c) fail-safe encryption

71.— Steganography often employs encryption to
a) hide information-theoretical information
b) reduce observed redundancy
c) add integrity protection

72.— Hybrid cryptosystems denote
a) application of both public- and symmetric-key systems
b) combinations of multiple block ciphers
c) stream ciphers with block-cipher-like features

73.— Differential cryptanalysis is kind of
a) hypothetical attack
b) known-plaintext attack
c) brute-force attack

74.— Authentication must be always bound to
a) a nonce
b) a session
c) a key

75.— Shamir's secret sharing scheme is secure in the
a) probabilistic sense
b) computational sense
c) information-theoretic sense

76.— The Shannon entropy corresponding to a roll of six-faced dice is
a) 2.718
b) 2.585
c) 6

77.— Message integrity could be compared to
a) signing documents
b) using invisible ink
c) putting letters inside an envelope

78.— Secret reconstruction in Shamir's secret sharing scheme involves solving
a) a linear equation system
b) a real-valued matrix inversion problem
c) a nonlinear equation system

79.— A pseudo-random sequence
a) cannot be very long
b) looks statistically random
c) cannot be predicted even theoretically

80.— The security of RSA is based directly on the difficulty of
a) calculating discrete logarithms
b) finding points on an elliptic curve
c) factoring large numbers

81.— If an LFSR has a maximum period and is of length n, then the period is
a) 2^{n-1}
b) 2^n
c) $2^n - 1$

82.— Two-round Feistel network
a) cannot be secure
b) is okay
c) is secure if the f-function is chosen with care

83.— The probability for a 1024-bit number being a prime is around
a) 710^{-1}
b) $710^{-1} \times 10^{-10}$
c) $710^{-1} \times 10^{-20}$

84.— If H is a subgroup of G, then
a) $|H| - 1$ divides $|G| - 1$
b) $|H|$ divides $|G|$
c) $|H|$ and $|G|$ are relative primes

85.— Euler's Theorem stats that $a^{\varphi(n)} \equiv 1 \pmod{n}$ when
a) $\gcd(\varphi(n), n) = 1$
b) $\gcd(a, n-1) = 1$
c) $\gcd(a, n) = 1$

86.— The size of $\mathbb{Z}_n^*$ equals
a) $\phi(n)$
b) $n - 1$
c) n

87.— Assume that you do two DSA signatures with the same secret parameter k. An enemy can then
a) recover the signed message
b) only recover the value of the secret parameter
c) recover the secret signing key

88.— The Diffie-Hellman parameters are chosen as $N = 2207$ and $g = 2$, and Alice and Bob have chosen the secret keys $a = 2$ and $b = 3$. The shared secret material will be
a) 12
b) 32
c) 64

89.— DSA stands for
a) Digital Signature Algorithm
b) Domestic Signing Algorithm
c) Data Security Amendment

90.— MAC stands for
a) Message Authentication Code
b) Manipulation Authorization Code
c) Markovian Algorithmic Coefficient

91.— IDEA is
a) an asymmetric cryptosystem
b) a block cipher
c) a stream cipher

92.— $\gcd(15, 17)$ equals to
a) 0
b) 2
c) 1

93.— If $n = pq$ is a product of two distinct primes, then $\varphi(n)$ equals
a) $(p-1)(q-1)$
b) $pq-1$
c) pq

94.— If G is a group and $x \in G$, then $\langle x \rangle$ is
a) an element of G
b) a subgroup of G
c) the group G

95.— A box outputs long random bit strings whose every bit is individually chosen, the probability of the one bit being $\frac{1}{3}$. The rate of the output language is
a) 0.633
b) 0.918
c) 1.585

96.— Disavowal protocols are related to
a) undeniable signatures
b) zero knowledge proofs
c) key distribution protocols

97.— Confidentiality denotes preserving
a) secrecy
b) authenticity
c) content

98.— LFSR stands for
a) Linear Feedback Secured Randomness
b) Linear Feedback Shrinking Rotator
c) Linear Feedback Shift Register

99.— The Diffie-Hellman key exchange's security depends on the intractability of the
a) graph isomorphism problem
b) integer factoring problem
c) discrete logarithm problem

100.— In a (t, n)-threshold scheme, to reconstruct a secret, you need at least
a) n shares
b) $n - t$ shares
c) t shares

101.— The certification model of PGP is
a) centralized
b) hierarchical
c) distributed

102.— $\gcd(15, 20)$ equals to
a) 3
b) 5
c) 10

103.— A hash function h is used to digest message prior to them being signed digitally. h must necessarily be
a) one-way
b) one-way and strongly collision resistant
c) one-way and weakly collision resistant

104.— A typical Feistel network can be described by the transformation
a) $(L, R) \longrightarrow (L \oplus f(R), R)$
b) $(L, R) \longrightarrow (R, L \oplus f(R))$
c) $(L, R) \longrightarrow (R, R \oplus f(L))$

105.— A certificate is
a) a signed statement
b) a signature
c) a public key

106.— The output length of SHA is
a) 128 bits
b) 160 bits
c) 80 bits

107.— $18^{200000} \bmod 19$ equals to
a) 14
b) 0
c) 1

108.— Transmission secrecy could be compared to
a) using invisible ink
b) signing documents
c) putting letters inside an envelope

109.— Typically applying digital steganography involves
a) replacing a message channel with random noise
b) creating a model of the most significant non-random components of some data stream
c) replacing a channel that carries random noise with a message

110.— The Prisoner's Problem is related to
a) steganography
b) identification methods
c) confidentiality

111.— The big problem with electronic voting is
a) ensuring that the voting humans are not under pressure
b) ensuring that the voting machinery has not been tampered with
c) ensuring that the voting system manages votes honestly

112.— The Rabin-Miller test is a test for
a) primality
b) weak Diffie-Hellman moduli
c) zero-knowledge property

113.— The Kerkhoff Principle is that
a) the encryption and decryption keys are the same
b) there does not exist a provably secure storage for encryption keys
c) the encryption algorithm must be assumed publicly know

114.— One of the operators used in the IDEA cipher is
a) multiplication modulo 2^{16}
b) addition modulo 2^{16}
c) multiplication modulo 2^{32}

115.— Subliminal channels are related to
a) stream ciphers
b) digital signatures
c) steganography in audio data

116.— Double encryption is suspectible to an attack that has the name
a) meet-in-the-middle
b) meet-the-man
c) man-in-the-middle

117.— A nonrepudiable transaction is a transaction that
a) cannot be later proved to have taken place
b) cannot be denied later by its originator
c) cannot be denied without interactive protocols

118.— Solving $2+7 \equiv x \pmod 5$ yields
a) $x \equiv 0 \pmod 5$
b) $x \equiv 1 \pmod 5$
c) $x \equiv 4 \pmod 5$

119.— The quantitative unit of information is
a) a bit
b) an entropy
c) a probability distribution

120.— Euler's Theorem is a generalization of
a) Fermat's Little Theorem
b) Fermat's Great Theorem
c) Chinese Remainder Theorem

121.— Assume $a|b$ and $b|c$. Then
a) $a|c$
b) $b|a$
c) $c|a$

122.— In RSA, if m encrypts to c and m' to c', then mm' encrypts to
a) $m^e + \binom{}{e1} m^{e-1}m' + \cdots + \binom{}{ee-1} mm'^{e-1} + m'^e$
b) cc'
c) $c + c'$

123.— IKE stands for
a) Implicit Key Expiration
b) Internet Key Exchange
c) Involutive Key Ensemble

124.— A necessary condition for the equation $x_1a + x_2b = 1$ having an integral solution (a, b constants) is that
a) x_1 and x_2 are relatively prime numbers
b) x_1 and x_2 are prime numbers
c) $\gcd(x_1, x_2) > 1$

125.— If the distribution of a random variable becomes "more flat", then its entropy
a) decreases
b) increases
c) could either increase or decrease

126.— RSA modulus is $1189 = 29 \cdot 41$. The secret exponent d is obtained by
a) inverting e modulo 1120
b) inverting e modulo 1160
c) inverting e modulo 1189

127.— The shared secret in the Diffie-Hellman key exchange has the form of
a) $g^{(a^b)}$
b) g^{a+b}
c) g^{ab}

128.— A plain Diffie-Hellman key exchange is suspectible to the
a) cut-and-choose attack
b) man-in-the-middle attack
c) discrete logarithm attack

129.— Let p be a prime number. Then the equation $x^2 \equiv a \pmod p$ for constant a has
a) either two or no solutions
b) from zero to two solutions
c) always a unique solution

130.— The best encryption method for tolerating individual bit errors is
a) a self-synchronous stream cipher
b) a synchronous stream cipher
c) a block cipher

131.— A hash function h is used to digest message prior to timestamp it by publishing the hash value. h must necessarily be
a) strongly collision resistant
b) one-way
c) weakly collision resistant

132.— RSA stands for
a) Rivest, Shamir and Adleman
b) Rabin, Salkovitch and Appersmith
c) Ronald, Sergei and Andreas

133.— The simple protocols for secure coin flipping are based on
a) probabilistic arguments
b) certificates
c) forward commitment