以下の各項目に対して、正しい場合は○、間違っている場合は×を書け。

(1) アリス・ボブ記法とは、プロトコルにおけるメッセージのやり取りを記述する簡潔な方法である。
(2) 暗号スイーツのスイーツとスイートルームのスイートは語源を同じくしている。
(3) Dolev-Yao モデルとは、確率的多項式時間チューリング機械を特徴づけるモデルである。
(4) SSL に対する million message attack は、記号論的に解析することが可能である。
(5) ノンス(NONCE)とは、Number (used) ONCE のことである。
(6) 記号論的モデルにおいて、元来の Needham-Schroeder の認証プロトコルは、中間者攻撃が可能であるため、レスポンダによるイニシエータの認証性を満たさないが、イニシエータによるレスポンダの認証性は満たす。
(7) プロトコルの検証において、記号論的解析と計算論的解析を融合する手法は間接的手法と直接的手法に大別されるが、直接的手法で証明できることは、間接的手法でも証明できる。
(8) 暗号化スキームを特徴づけるゲームには引き分けがない。
(9) セキュリティ・パラメタとは、秘密鍵を生成する際に使われるパラメタのことである。
(10) 関数 $f(n)$ が negligible でない場合、多項式 $p(n)$ と自然数 N が存在して、$n>N$ ならば常に $f(n)>1/p(n)$ が成り立つ。
(11) IND-CCA1 安全な暗号化スキームは、IND-CCA2 安全である。
(12) AES よりも DES の方が安全性が高い。
(13) 疑似乱数から作られた private-key の暗号化スキームは、IND-CCA2 安全性を満たさない。
(14) アンサンブル X と Y が多項式時間識別不能であるならば、多項式時間サンプリングにより識別不能である。
(15) ランダムな文字列の書かれたテープを(確率的でない)チューリング機械に入力として与えることにより、確率的チューリング機械を実現することができる。
(16) オラクルとは、チューリング機械の停止性を判定する手続きのことである。
(17) Needham-Schroeder の認証プロトコルにおいて、イニシエータが一人で、レスポンダが存在しない場合、用いられている暗号化スキームが IND-CPA を満たせば、レスポンダになりすますことはできない。
(18) 暗号化スキームに関する仮定からプロトコルの安全性を示すには、暗号化スキームに対する攻撃者からプロトコルに対する攻撃者を構成すればよい。
(19) Type0 の暗号化スキームのもと、$\{\{0\}_K, K\}$ と $\{\{0,0\}_K, K\}$ は等価である。
(20) Abadi-Rogaway の証明において、ハイブリッド論法が可能であるのは、暗号の循環がないと仮定されているからである。

（裏面あり）

(21) Mapping Lemma によって、任意の記号論的トレースに対して、それに対応する計算論的トレースが存在することが保証される。

(22) ランダムネス記号は、記号論的モデルにおいて、暗号化や署名の際に導入されたランダムネスを表している。

(23) ストランド空間において、ノンスは唯一の起源を持つ。

(24) ストランド空間を用いて認証性を示すには、特定の参加者のストランドの存在を仮定して、攻撃者のストランドが存在しないことを証明すればよい。

(25) Protocol Composition Logic の honesty rule はプロトコルには依存しない。

(26) 5 分間大学は Father Guido Sarducci の十八番である。

(27) Hoare 論理において、{P} S {Q} という三つ組は、条件 P のもとで S が停止しない場合には、成り立たない。

(28) 確率Hoare論理において、{ P(true)=1 } x := 0 $\oplus_{1/3}$ (x := 1 $\oplus_{1/2}$ x := –1) { P(x=–1)=1/3 } は成り立つ。

(29) DDH 仮定により、ElGamal 暗号の IND-CCA2 安全性が導かれる。

(30) 次の確率プロセス計算の等価性の右辺において、r の値は、x の値とは全く独立にランダムに設定される。

$$
\begin{aligned}
&\textbf{foreach } i_{\mathrm{h}} \leq n_{\mathrm{h}} \textbf{ do } OH(x : bitstring) := \textbf{return}(\mathsf{hash}(x)) \\
\approx_0 &\textbf{foreach } i_{\mathrm{h}} \leq n_{\mathrm{h}} \textbf{ do } OH(x : bitstring) := \\
&\quad \textbf{find } u \leq n_{\mathrm{h}} \textbf{ suchthat } (\textbf{defined}(x[u], r[u]) \wedge x = x[u]) \textbf{ then return}(r[u]) \\
&\quad \textbf{else } r \xleftarrow{R} D; \textbf{return}(r)
\end{aligned}
$$

解答用紙

学生証番号 _____ 氏名 _____

(1)		(2)		(3)		(4)		(5)	
(6)		(7)		(8)		(9)		(10)	
(11)		(12)		(13)		(14)		(15)	
(16)		(17)		(18)		(19)		(20)	
(21)		(22)		(23)		(24)		(25)	
(26)		(27)		(28)		(29)		(30)	