Ukázkové otázky z KPB

Test bude mít 5 - 6 otázek.

1. Jakou velikost klíče K podporuje algoritmus DES?
2. Je dán protokol, ve kterém odesílatel (Alice) vykonává následující operace:
   Protokol: $c = e_K(m||sig_{K_s}(H(m)))$,
   kde sig_{K_s} je dig. podpis prostřednictvím soukromého klíče K_s, K je tajný klíč.
   Jaké operace (kroky) bude provádět příjemce (Bob) poté, co obdrží zprávu c?
3. Jaký je prostor klíčů pro Polyboisovu šifru? Zdůvodněte.
4. Tvrzení: Faktorizace a 700-bitového RSA modulu je v současnosti mimo možnosti počítačových technologií. Je toto tvrzení pravdivé?
5. Nalezněte dvojice čísel, která jsou navzájem inverzní modulo 11 vzhledem k operaci násobení.
6. Pro design blokových symetrických algoritmů jsou důležité mnohé vlastnosti. Vysvětlete dvě z nich:
   (a) Lavinový (Avalanche) efekt
   (b) Úplnost (Completeness)
7. Popište protokol Diffie-Hellman pro ustavenní klíče.
8. Co je to certifikát veřejného klíče? K čemu slouží a jaká je jeho struktura (co obsahuje)? Kdo ho vydává, a které údaje na certifikátu souvisí s vydavatelem certifikátu?
9. Popište režim Counter Mode (režim čnnosti symetrických šifrovacích algoritmů). Jak se šifruje, dešifruje, výhody, nevýhody,....
10. Jaké vlastnosti musí mít generátory pseudonáhodných sekvencí pro kryptografické účely?