Help-sheet for Cryptography

Alphabet.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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

κ-values.

German: $\kappa_D = 0,0762$, English: $\kappa_E = 0,0669$, French: $\kappa_F = 0,0746$.

RSA.

Public key:	$(n, e) \in \mathbb{N} \times \mathbb{Z}^*_{\varphi(n)}$,
	$n = pq$, $p \neq q$ prim,
Private key:	$d = e^{-1} \mod \varphi(n)$,
Message:	$m \in \{1, \dots, n-1\}$,
Encryption:	$c = m^e \mod n$,
Decryption:	$m = c^d \mod n$.

Rabin.

Public key:	$n = pq$ for primes $p \neq q$,
	$p, q \equiv 3 \pmod 4$,
Private key:	(p, q),
Message:	$m \in \{1, \dots, n-1\}$,
Encryption:	$c = m^2 \mod n$,
Decryption:	find square roots modulo n.

ElGamal.

System parameters:	prime p,
	Generator a modulo p,
Private key:	$x \in \{2, \dots, p-2\}$,
Public key:	$y = a^x \mod p$,
Message:	$m \in \{1, \dots, p-1\}$,
Encryption:	choose random $k \in \{2, \dots, p-2\}$,
	$K = y^k \mod p$,
	$c_1 = a^k \mod p$,
	$c_2 = Km \mod p$,
	$c = (c_1, c_2)$,
Decryption:	$K = c_1^x \mod p$.
	$K^{-1} = c_1^{p-1-x} \mod p$,
	$m = K^{-1} c_2 \mod p$.

Goldwasser-Micali.

Public key:	$n = pq$ for $p \neq q$ prime,
	$y \in \mathbb{Z}_n$ pseudosquare modulo n,
Private key:	(p, q),
Message:	$m = (m_1, \dots, m_t) \in \{0,1\}^t$,
Encryption:	choose independent random numbers
	$x_1, \dots, x_t \in \mathbb{Z}^*_n$,
	$c_i = \begin{cases} y x_i^2 \mod n, & \text{if } m_i = 1, \\ x_i^2 \mod n, & \text{if } m_i = 0, \end{cases}$
	$i = 1, \dots, t$.
	$C = (c_1, \dots, c_t)$,
Decryption:	
	$m_i = \begin{cases} 0, & \text{if } (\frac{c_i}{p}) = 1, \\ 1, & \text{else}, \end{cases}$
	$i = 1, \dots, t$,
	$m = (m_1, \dots, m_t)$.

Blum-Goldwasser.

Public key:	$n = pq$ for primes $p \neq q$,
	$p, q \equiv 3 \pmod 4$,
Private key:	(p, q, a, b) with $ap + bq = 1$,
Message:	$m = (m_1, \dots, m_t) \in \{0,1\}^{ht}$
	with $h \leq \log_2 \lfloor \log_2 n \rfloor$,
Encryption:	choose random QR x_0 modulo n,
	$x_i = x_{i-1}^2 \mod n$, $i = 1, \dots, t+1$,
	b_i: last h bits of x_i,
	$c_i = m_i \oplus b_i$, $i = 1, \dots, t$,
	$C = (c_1, \dots, c_t, x_{t+1})$,
Decryption:	$d_1 = (\frac{p+1}{4})^{t+1} \mod (p-1)$,
	$d_2 = (\frac{q+1}{4})^{t+1} \mod (q-1)$,
	$u = x_{t+1}^{d_1} \mod p$, $v = x_{t+1}^{d_2} \mod q$,
	$x_0 = vap + ubq \mod n$,
	$x_i = x_{i-1}^2 \mod n$, $i = 1, \dots, t+1$,
	b_i: last h bits of x_i,
	$m_i = c_i \oplus b_i$, $i = 1, \dots, t$,
	$m = (m_1, \dots, m_t)$.

ElGamal-Signatures.

System parameters:	prime p,
	Generator a modulo p,
Private key:	$x \in \{2, \dots, p-2\}$,
Public key:	$y = a^x \mod p$,
Hash function:	$h : \{0,1\}^* \to \{1, \dots, p-1\}$,
Document:	$m \in \{0,1\}^*$,
Signature:	choose random $k \in \{2, \dots, p-2\}$,
	$\gcd(k, p-1) = 1$,
	calculate $r = a^k \mod p$,
	$k^{-1} \mod (p-1)$, $h(m)$,
	$s = k^{-1}(h(m) - xr) \mod (p-1)$
	the signature of m is (r, s),
Verification:	check $1 \le r \le p-1$,
	$v_1 = y^r r^s \mod p$,
	$v_2 = a^{h(m)} \mod p$,
	accept, if $v_1 = v_2$.

DSA.

System parameters:	primes p, q with $q \mid p-1$,
	$a \in \mathbb{Z}_p^*$ element of order q,
Private key:	$x \in \{2, \dots, q-1\}$,
Public key:	$y = a^x \mod p$,
Hashfunction:	$h : \{0,1\}^* \to \{1, \dots, q\}$,
Document:	$m \in \{0,1\}^*$,
Signature:	choose random $k \in \{2, \dots, q-1\}$,
	calculate $r = (a^k \mod p) \mod q$,
	$k^{-1} \mod q$, $h(m)$
	$s = k^{-1}(h(m) + xr) \mod q$
	the signature of m is (r, s),
Verification:	check $0 < r < q$ and $0 < s < q$,
	calculate $w = s^{-1} \mod q$ and $h(m)$,
	$u_1 = wh(m) \mod q$, $u_2 = rw \mod q$,
	$v = (a^{u_1} y^{u_2} \mod p) \mod q$,
	accept, if $v = r$.

Feige-Fiat-Shamir-Identification.

System parameters:	primes $p \neq q$, $p, q \equiv 3 \pmod 4$,
	TA publishes $n = pq$,
	each user chooses $s_1, \dots, s_k \in \{1, \dots, n-1\}$,
	$\gcd(s_i, n) = 1$,
	and publishes $v_i = (s_i^2)^{-1} \mod n$, $i = 1, \dots, k$,
Protocol:	A chooses random r,
	calculates $x = r^2 \mod n$,
	$A \to B$: x,
	B chooses random bits $b_1, \dots, b_k \in \{0,1\}$,
	$A \leftarrow B$: $(b_1, \dots, b_k)$,
	A calculates $y = r \prod_{j=1}^{k} s_j^{b_j} \mod n$,
	$A \to B$: y,
	B calculates $z = y^2 \prod_{j=1}^{k} v_j^{b_j} \mod n$,
	accepts, if $z = x$.

Addition rules for elliptic curves.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2) \in E(L)$ for $L \supseteq K$.

(i) If $P_1 \neq \pm P_2$, than $P_1 + P_2 = (x_3, y_3)$ with

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2,$$
$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1,$$

(ii) if $P_1 \neq -P_1$, than $2P_1 = P_1 + P_1 = (x_3, y_3)$ with

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1,$$
$$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1.$$